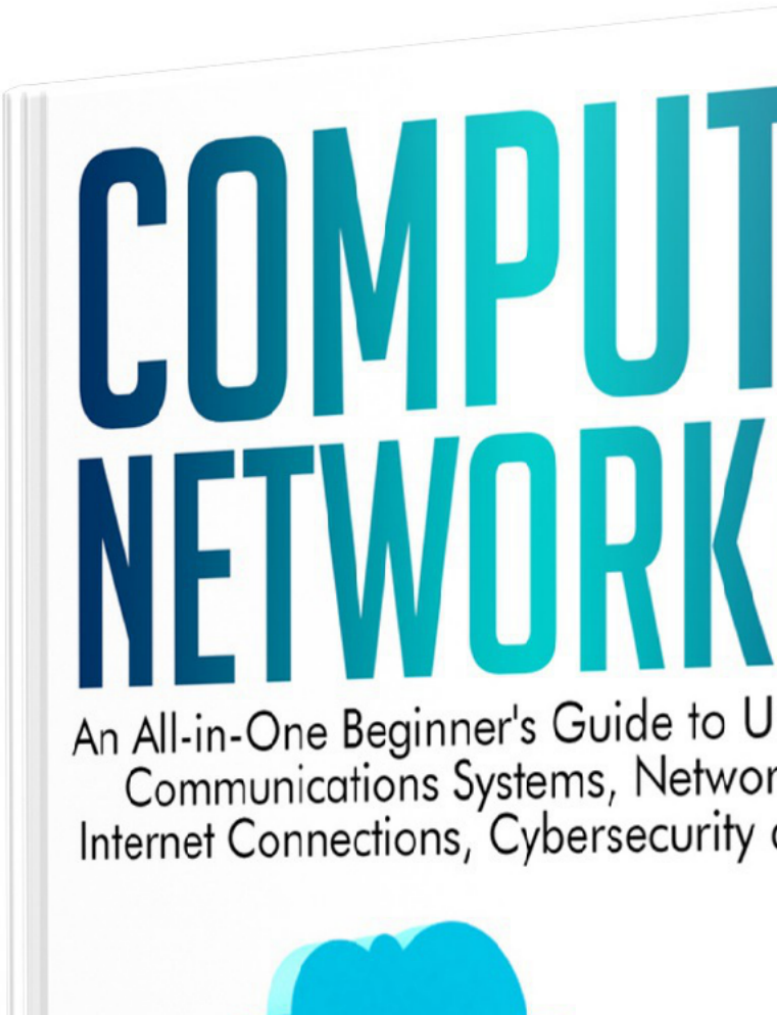

COMPUT
NETWORK
An All-in-One Beginner's Guide to U
Communications Systems, Networ
Internet Connections, Cybersecurity

Computer Networking and Cybersecurity

A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats

© Copyright 2020
All Rights Reserved. No part of this book may be reproduced in any form without permission in writing from the author. Reviewers may quote brief passages in reviews.

Disclaimer: No part of this publication may be reproduced or transmitted in any form or by any means, mechanical or electronic, including photocopying or recording, or by any information storage and retrieval system, or transmitted by email without permission in writing from the publisher.

While all attempts have been made to verify the information provided in this publication, neither the author nor the publisher assumes any responsibility for errors, omissions or contrary interpretations of the subject matter herein.

This book is for entertainment purposes only. The views expressed are those of the author alone, and should not be taken as expert instruction or commands. The reader is responsible for his or her own actions.

Adherence to all applicable laws and regulations, including international, federal, state and local laws governing professional licensing, business practices, advertising and all other aspects of doing business in the US, Canada, UK or any other jurisdiction is the sole responsibility of the purchaser or reader.

Neither the author nor the publisher assumes any responsibility or liability whatsoever on the behalf of the purchaser or reader of these materials. Any perceived slight of any individual or organization is purely unintentional.

Contents

Part 1: Computer Networking
Introduction
Chapter 1: Computer Networking Basics
What is Modern Computer Networking?
Chapter 2: Networking Services Explained
Domain Name System (DNS)
Dynamic Host Configuration Protocol (DHCP)
Hypertext Transfer Protocol (HTTP)
File Transfer Protocol (FTP)
Network News Transfer Protocol (NNTP)
Simple Mail Transfer Protocol (SMTP)
Keeping the Networks Safe with Firewalls
Chapter 3: Getting into the Networking Hardware
Fundamentals of Computer Relationships
Core Hardware Elements of a Network
Servers
Hubs, Switches, and Routers
Cabling and Cable Plants
Workstation Hardware
Utilizing the Network Traffic and Knowing the Network Hardware
Repeaters
Hubs (Concentrators)
Switches
Bridges
Routers
Gateways
The Core Fundamentals of Cable Topologies
Star Topology
Ring Topology
Chapter 4: Wireless Communication Systems and Connecting to the Internet
Connecting to the Internet
Wide Area Networks
Internet and Intranet
Understanding the Features of Networking
File Sharing
Printer Sharing
Application Services
E-mail
Remote Access
Chapter 5: Common Network Protocols and Ports
TCP/IP and UDP
Domain Name System (DNS), allowing users to access websites with easy-

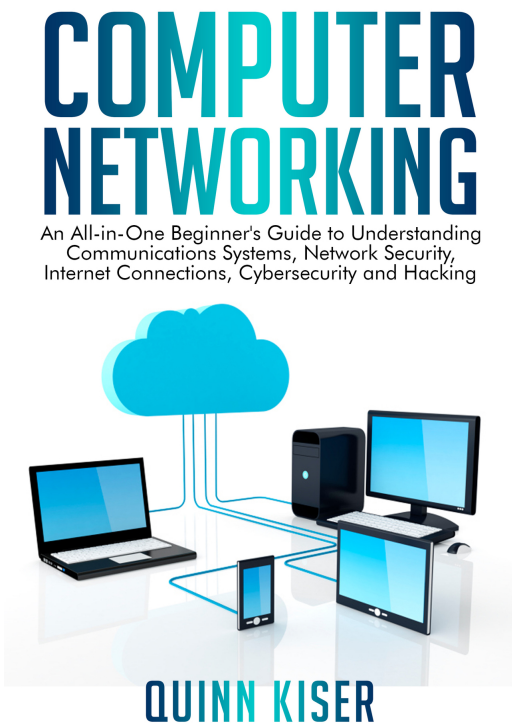
to-remember domain names instead of long numerical IP addresses.
Dynamic Host Configuration Protocol (DHCP), for assigning TCP/IP addresses to the nodes in a network.
Hypertext Transfer Protocol (HTTP), which controls the transfer of data between the client and the webserver.
File Transfer Protocol (FTP), which defines the method by which file data is sent and received between the FTP client and the FTP server.
Network News Transfer Protocol (NNTP), specifically used for Usenet discussion groups on the Internet.
Simple Mail Transfer Protocol (SMTP), which handles the sending and receiving of e-mails from one e-mail server to another.
Chapter 6: Learning About the OSI Networking Model
Layer 1: The Physical Layer
Layer 2: Data-Link Layer
Layer 3: Network Layer
Layer 4: Transport Layer
Layer 5: Session Layer
Layer 6: Presentation Layer
Layer 7: Application Layer
Chapter 7: Network Security, Cybersecurity, and Hacking Methods
Account Security
Password Security
File and Directory Permissions
Practices and User Education
Understanding External Threats
Front-Door Threats
Back-Door Threats
DDoS Threats
Potential Attacks and Threats
Basics to Hacking and Network Design
The Process of Designing a Network
Assessing Network Needs
Applications
Users
Network Services
Meeting the Network Needs
The Basics of Hacking: The Kill Chain Process
Phase 1: Reconnaissance
Phase 2: Intrusion
Phase 3: Exploitation
Phase 4: Privilege Escalation
Phase 5: Lateral Movement
Phase 6: Obfuscation
Phase 7: Denial of Service
Phase 8: Exfiltration
Chapter 8: Useful Cybersecurity Tips for 2020

Vital Function of a Disaster Recovery Plan
Assessing Disaster Recovery Needs
Considering Disaster Scenarios
Assessing Backup Needs
Acquiring Backup Media and Technologies
Choosing Backup Strategies
Conclusion
Part 2: Cybersecurity
Introduction
Chapter One: Cybersecurity and Why It's Important
What is Cybersecurity?
Why is Cybersecurity Important?
Cybersecurity Scenarios
Cybersecurity Terminology
History of Cyberattacks
Chapter Two: Cyberattacks and 10 Types of Cyber Hackers
Classification of Cybercrimes
Reasons for Cybercrimes
Types of Cyber Hackers
Common Tools Used by Hackers
Types of Cybercrime
Chapter Three: Recognizing and Countering a Phishing Attack
What is Phishing?
Methods used for Phishing
Common Ways to Tackle Phishing Attacks
Types of Phishing and How to Protect Yourself against Them
Identifying a Phishing Email
Identifying a Spoofed Email
Chapter Four: How to Identify and Remove Malware
Types of Malware
Protecting Yourself from Malware
Chapter Five: Recovering from Ransomware
Defining Ransomware
Types of Ransomware
Chapter Six: How to Spot and Stop a Social Engineering Attack
Social Engineering Methodologies
Spotting a Social Engineering Attack
How to Avoid Falling for Social Engineering
Tips
Look out for Banking Scams
Chapter Seven: Network Security and Protection Techniques
Network Security
How Does the Network Security Function?
Top Five Attacks Through a Network that can Affect Your Business
Protecting your Business from a Cyber Attack

Cybersecurity through Configurations and Settings
Some Tips to Maintain Cybersecurity
Chapter Eight: Web Application and Smartphone Security
Web Application Security
How Can You Secure Web Applications?
Chapter Nine: 9 Security Testing Methods
Types of Security Testing
Types of Penetration Testing
Chapter Ten: Skills Required for a Career in Cybersecurity
Entry-Level Roles
Senior Level Roles
Four Popular Careers in Cybersecurity and How to Get There
Required Skillset for a Career in Cybersecurity
Technical Skills
Conclusion
References

Part 1: Computer Networking

An All-in-One Beginner's Guide to Understanding Communications Systems, Network Security, Internet Connections, Cybersecurity and Hacking



Introduction

This book is a concoction of several computer topics that are relevant and popular in the modern age. Throughout this book, the reader will explore each topic with easy-to-understand terminology and analogies. The book starts with a descriptive and comprehensive insight into computer networking and then branches off to cover network security, network designing, and hacking. The delivery of topics is specifically designed to:

- Entertain the needs of the readers.
- Provide valuable insights into the world of computer networking in the modern era.
- Deliver elaborative yet to-the-point knowledge.

Once the computer networking portion of this book is finished, the reader will be greeted with the other topics in this all-in-one guide. In the ending section, there is an informative description of the kill-chain process in hacking. This topic is not only interesting but also informative and refers to the methods hackers employ when penetrating target systems and networks. So, buckle your seatbelts and enjoy the ride.

Chapter 1: Computer Networking Basics

In this chapter, we will explore the fundamentals and the very basic concepts of computer networking. By doing so, we will essentially lay a conceptual foundation for the reader. This will help increase the digestibility of the later discussed concepts and some technical details of computer networking.

Hence, this chapter will be primarily focused on emphasizing the basic details of computer networking and then steadily building upon the knowledge as you learn.

To start things off, we will go through a brief introduction of what computer networking actually is. Then we will delve deeper into the details solidifying the understanding of each concept that the reader will have successfully learned.

What is Modern Computer Networking?

The word “networking” describes a connection or set of connections between multiple objects. Similarly, “computer networking” refers to the interconnection of two or more computers together to allow for sharing resources. A network of computers can be established in a variety of environments, such as homes, offices, or even in large business organizations. Computer networking stretches even to the international scope where computers are connected through the Internet. A more subtle and easily observed example of computer networking is a printer or a scanner connected (wired or wireless) to the user's personal computer.

Since the fundamental purpose of computer networking is to interconnect different PCs, an interesting question arises; why do we need computer networking in the first place?

The answer to this is very simple. If a person wants to watch a movie, a video, or even a talk show, he can do so in two ways.

- By having a physical storage device that contains the content, viewable on his computer, or simply by hopping onto the Internet and accessing the website where he can find the content and view it directly from there.

- The latter approach involves computer networking. It enables the viewer to connect to a remote computer server that is the host of the website allowing the visitor to use its resources to view his favorite content. This is just a simple example of how computer networking benefits an average user.

The phenomenon of the Internet is a by-product of computer networking, and we all know what it's like to spend a few days without the Internet. While we have discussed how big a deal computer networking is to a common person, it becomes even more important and crucial for big organizations and institutes such as hospitals, business companies, law enforcement departments, etc. These organizations rely on computer networking to:

- Efficiently establish an information channel through which the entire organization communicates the data being gathered and modified. Computer networking has a huge influence on not only the professional sector but also the business sector as well because, without a proper networking infrastructure, the respective industry would essentially just collapse.

Hence, to understand the importance and the very basic function of computer networking, note that computer networking is the very foundation of the Internet itself.

Transferring data from one place to another is the purpose of networking. Another important thing we have to know about any connection is how much data it can carry from one place to another. This capacity to carry data is called *bandwidth* . If a connection has a higher capacity bandwidth, it can carry more data within a specific time slot.

The rate at which a network can transfer data is measured in bits per second, which are abbreviated as 'Bps.' Bps means how many bits a bandwidth can carry per second. In the modern age, computer technology and networking have come a long way; this bandwidth capacity is now measured in multiples of thousands. The different measures of data transfer speed are:

- Kilobytes - thousands of bits per second (Kbps)
- Megabytes - millions of bits per second, or thousands

of Kilobytes per second (Mbps)

- Gigabytes - billions of bits per second, or thousands of Megabits per second (Gbps)

A closely related measurement you will also see in computer networking is ‘hertz’; it is the number of cycles being carried per second, in the same way ‘hertz’ expresses the number of cycles per second in an alternating-current signal. Hertz is abbreviated as ‘Hz’ and is used to measure the computational speed of a processor. This measurement is taken in multiples of thousands, and:

- A thousand Hertz is known as a kilohertz (kHz)
- A million Hertz is known as a Megahertz (MHz)
- A billion Hertz is known as a Gigahertz (GHz)

For example, a processor running at 100 MHz means 100 million cycles per second. Hz and bps are essentially the same measurement but used for different elements. However, sometimes they can be mixed up. For instance, saying that an Ethernet cable supports a 10 MHz bandwidth instead of 10 Mbps is acceptable in common usage.

Chapter 2: Networking Services Explained

In this section, we will discuss several network protocols that either rely on or make use of the TCP/IP protocol.

The protocols we will be discussing are listed below

1. DNS
2. DHCP
3. HTTP
4. FTP
5. NNTP
6. SMTP

There will be references to the levels at which these protocols operate in terms of the Open Systems Interconnection, or “OSI”, networking model. The OSI model defines most methods and protocols through which computers connect and communicate with each other on a network. It is an abstract visualization, but a useful one; understanding the OSI networking model will create a strong foundation for network designing and network solution engineering.

Chapter Six goes into a detailed treatment of the topic, but, purely for the sake of reference between here and there, we will merely present here a basic outline of the OSI model.

The model is divided into seven distinct and separate layers. Each layer possesses a trait known as ‘successive dependence.’ This means that the successively higher layers in the model depend largely on the services and characteristics of the preceding lower layers.

Consider a standard desktop computer system. It is composed of several components that must work together to make the system functional. If we divide this system into the layers of the OSI networking model, the hardware components of this computer will be termed as the ‘lowest layer.’ The next layer above the hardware layer of this computer would be the Operating System and its system drivers.

Obviously, the operating system and drivers would be useless

without the corresponding hardware. Hence, this higher layer is depending on the preceding lower layer to perform its function properly. This successive-hierarchy visualization continues upwards to the final layer, where an application is displaying useful and digestible data to the user.

The seven layers of the OSI Networking Model are:

1. **Physical Layer** – The physical layer specifies the network cable, the router, the DSU/CSU box, and the other physical mediums involved.
2. **Data Link Layer** –The data link layer of the OSI model bridges the connection between the third layer (network layer) and the first layer (physical layer) by defining and implementing a protocol through which the network layer transmits its data to the physical layer.
3. **Network Layer** – The main job of the network layer is to define the route through which the data packets will travel from node to node. For this purpose, the transport layer masks the characteristics of lower layers from the upper layers in the OSI model.
4. **Transport Layer** – The transport layer mediates the movement of data between all the other layers.
5. **Session Layer** – By this layer, the OSI model defines the connection between two computers as either a client-server connection or a peer-t0-peer connection. The term 'session' is used to describe this virtual network connection between computers.
6. **Presentation Layer** – The presentation layer performs data compression/ decompression and encryption/decryption.
7. **Application Layer** – The main concern of the application layer is to control and mediate the interaction of the network with the Operating System and the applications installed on this OS. It basically defines how the applications handle the communications in which the system becomes involved when connected to a network.

If we analyze the nature of the OSI-model layers in a network, we see that they begin their interaction with the physical elements within a network, i.e., the routers, network cables, etc. From there,

the layers move toward interacting with virtual features and elements, i.e., moving toward intelligent aspects of the network. After this, the OSI model's focus on the virtual aspects of the network shift towards the involvement of the computer machine itself within the network, which is evident from the last two layers (Presentation and Application layers).

A good grasp of this technique allows network engineers to analyze networks in a more detailed and comprehensive manner.

Domain Name System (DNS)

The Doman Name System was developed to solve the inherent problem of keeping track of websites' IP addresses on the Internet. For instance, let's say that you want to visit Google. If the server housing Google's resources had only an IP address, then you would have to type in **http://209.85.171.100** to access it. If the computer addresses on the Internet had the same addressing scheme, keeping track of them would be very difficult.

This is where DNS comes in. By using this system, people can register a name for their domain with ICANN. This registered name will access that IP address on the Internet. Here are some of the common domain extensions:

- **.edu** (used by educational institutions)
- **.gov** (used by governmental institutions)
- **.mil** (used by military institutions)
- **.net** (used by entities related to the Internet)
- **.org** (used by non-profit organizations)
- **.xx** (used by countries. The "xx" is a space-holder and is replaced by the respective country's initials. For instance, for America: ".us").

Once an entity has acquired a domain name, it may add descriptors into the domain name. For instance, for the domain **dirbs.gov** , the government entity can add **pta.dirbs.gov,** and it would be acceptable.

The names of the domains are resolved to their respective IP addresses by using DNS servers, which means 'domain-name servers'. These servers perform a database query against a domain name entered by the user. The server then returns the actual address of the domain to the user's web browser.

Dynamic Host Configuration Protocol (DHCP)

The DHCP protocol was developed to facilitate the administrators of a network to assign TCP/IP addresses to nodes easily. This protocol was used in a time when administrators would resolve the address of a node to a TCP/IP address and put it into a text file or even a dialog box.

The services given by the DHCP protocol is essentially run by dedicated servers known as DHCP servers. These servers control a 'scope,' which is an array of IP addresses. So, when a node goes online on a network, it requests the DHCP server to assign it an address. These addresses are valid for a limited period and expire after the time limit assigned; they then become available for another node to use. This period is known as the 'lease period,' and it can be set by the administrators of the network.

The main use of the DHCP protocol is to support the connectivity needs of client workstations. Using DHCP for the nodes responsible for network services is not recommended, as any change to the TCP/IP address will negate the connection to the network service.

Hypertext Transfer Protocol (HTTP)

The entire Internet (called the World Wide Web) is a collection of documents created using a formatting language known as 'HTML' or 'Hypertext Markup Language.' Hypertexts on the Internet usually consist of:

- Displayed text
- Graphical images
- Formatting commands
- Hyperlinks (clicking them redirects the user to some other document on the Internet)

HTML documents are commonly accessed by using web browsers such as Google, Chrome, and Safari.

The Hypertext Transfer Protocol is what controls the transfer of data between the client and the webserver. This protocol operates at the application layer of the OSI model. The HTTP protocol makes use of other Internet protocols and DNS to establish a connection between the web client and the webserver. The HTTP protocol itself is insecure because transferring data happens with no encryption and can be intercepted. To resolve this security issue, we now use

‘HTTP secure’, commonly known as HTTPS, and SSL (Secure Socket Layers).

File Transfer Protocol (FTP)

The word FTP refers to both 'File Transfer Protocol' and 'File Transfer Program,' both of which are related to each other in that the latter is an application that makes use of the FTP protocol. However, in this section, we will only discuss the FTP protocol.

FTP performs at the application layer in the OSI model, and it defines the method by which file data is sent and received between the FTP client and the FTP server. The data transferred can be text-based or binary-based, and there is no limit on the file size FTP can handle.

To perform a file transfer, the user must first connect to the FTP server and log in with a valid username and password. Some sites allow users to enter the username 'anonymous' with their e-mail address being the password. This is known as 'Anonymous FTP.'

Network News Transfer Protocol (NNTP)

This protocol is specifically used for Usenet. Usenet is a term referring to discussion groups on the Internet. These groups cover a huge variety of topics, and at the moment, there over ten thousand Usenet groups on the Internet. The conversations of a Usenet group are sent to the Usenet servers, which are then sent to the other international Usenet servers by echoing.

Several classifications of Usenet groups are:

- **Alt:** Usenet group that focuses on topics on alternate lifestyles and miscellaneous issues.
- **Comp:** Usenet group that focuses on computer topics.
- **Gov:** Usenet group that focuses on discussions about governments.
- **Rec:** focus on recreational topics.
- **Sci:** focus on discussions about science.

Usenet groups are not all public. Those groups that are public get the news echoed by other Usenet servers, but the private ones are generally hosted by some organization or institution. Private Usenet groups require users to authenticate themselves with proper usernames and passwords.

The phenomenon of Usenet is made possible only by the NNTP protocol. This protocol establishes a connection between the Usenet server and the Usenet reader. The protocol also handles message formatting. This makes it possible for the messages to be text-based or carry binary attachments. Messages with binary attachments are encoded through MIME, or Multipurpose Internet Message Encoding (the same encoder used for e-mail attachments).

Simple Mail Transfer Protocol (SMTP)

The Simple Mail Transfer Protocol handles the sending and receiving of e-mails from one e-mail server to another. The SMTP protocol is simply a way to communicate with the sending and receiving systems of e-mail servers.

The SMTP protocol comes into play when the system sending the e-mail message connects to the receiving system through port 25. Once the connection between the two systems has been established, the sender then transmits a '**HELO** ' command along with its respective address towards the receiving system. Once this command has been acknowledged, and the receiver responds with its own address, then communication is initiated. The sender can then issue a command indicating it wants to send a message, by specifying the intended recipient of the message. Once the receiving system gets this request, it looks for the recipient. If the recipient is known to the system, then the request is acknowledged, and the sending system then forwards the message, along with any attachments, to the recipient. Once the receiving system has acknowledged that the entire message has been received, it terminates the connection.

Keeping the Networks Safe with Firewalls

Most people reading this book would have come across the Windows firewall prompt at least once. This firewall application running on your machine is what keeps the network security policies upheld. Firewalls are hardware devices that protect a network by enforcing the network's security policies. In most networks, a firewall is installed into the router itself, leveraging its micro-processing chip and built-in memory. This is true with networks designed and installed in small offices or similar scenarios. However, for large networks, the networking equipment includes dedicated hardware running the firewall. This hardware

can be a single unit or multiple pieces.

Normally, a separate computer running the firewall software is designated for the network. Otherwise, there can be a firewall device with a computer chip within it. Generally, a firewall acts as an outpost stationed between a LAN and the Internet. Regarding the firewalls available for use, there are mainly two types:

1. **Network-Based Firewall:** This firewall operates at the third layer, also known as the data-link layer, of the OSI networking model. The security technique used by a network-based firewall is primarily 'packet filtering.' Using this technique, the firewall is programmed with a defined set of rules. Whenever data packets travel between the two networks, the firewall analyzes and compares this packet against the rules and then decides whether the packet should be allowed to arrive or depart from the network or not. The permission or denial of passage according to the packet-filtering rules for the data packets is usually based on their destination address, source address, or the TCP/IP port.
2. **Application Based Firewall:** This firewall serves the role of a proxy. The word 'proxy' in this context means that the firewall represents the user's interactive session with the server of which services are requested. An application-based firewall allows no data traffic to pass through the two networks directly. Instead, the communication between the two networks will be handled on one side by the firewall, as a proxy. This is why an application-based firewall is also known as a 'proxy firewall.' The technique used by a proxy firewall is 'NAT,' also known as 'Network Address Translation.' In this technique, the main idea is to conceal the network addresses of the internal network so it is not directly visible to the external network. In an application-based model, the firewall is responsible for the transmission of data to the network addresses for which the connections are established.

Chapter 3: Getting into the Networking Hardware

Fundamentals of Computer Relationships

The term ‘computer relationship’ refers to how a computer interacts with another computer connected on a network. There are generally two types of computer relationship.

1. **Peer to Peer**
2. **Client/server**

These two types of relationships essentially define the logical structure of a network. To understand them better, make an analogy to different management philosophies.

A peer-to-peer, or ‘P2P’, network is much like a decentralized management philosophy where decisions are made locally, and resources are managed according to what users need to do first.

A Client/server network is almost like a company that uses centralized management where decisions are made in a central location within a group of a few people. There exist circumstances where P2P and client/server relationships are both appropriate, and many networks incorporate both in their setup.

Both P2P and client/server networks need certain layers in the OSI model to be common, along with a physical network connection between the communicating computers using the same network protocols. In this respect, the two types of computer relationships are virtually the same in a network. However, the major difference arises from whether you spread the shared network resources around all the computers on the network or use the centralized network servers.

Core Hardware Elements of a Network

To reinforce and solidify the foundation of the concepts we are exploring in this discussion, you must learn more about the physical hardware components that make up a computer network. Until

now, we have focused more on how a network works and interacts on the virtual level rather than the physical level. However, by understanding the behavior of the network in its virtual realm, we are now set up to understand the hardware.

Understanding the physical aspect of computer networks provides us with adequate knowledge by which we can not only set up a computer network properly but also troubleshoot and maintain it.

In this section we will be discussing the following hardware, each a core component of the network:

1. Servers
2. Hubs
3. Routers
4. Switches
5. Cabling and cable plants
6. Workstation hardware

In the ending sections of this chapter, we will discuss these hardware components within the context of directing network traffic. However, we will only focus on understanding these components and their purposes.

Servers

A server is a computer assigned a very important and demanding job in computer networking. A server computer is essentially the component that handles all the networking requests and other functions of the computers on the network. Based on the network functions, a server can be classified into these different categories.

- **File and Print Servers:** This category includes those servers that primarily provide file-sharing services to other computers, and handle requests for network-based printers.
- **Application Servers:** The servers that essentially provide specific network application services to programs and software fall under this category. For example, a server running a database can provide (on request) access to the database to a distributed application connected to this server.
- **E-mail Servers:** The servers primarily designed to store e-mails and provide interconnection services to

the corresponding clients are categorized as ‘E-mail Servers.’

- **Networking Servers** : This category of servers mainly offers a variety of services related to networking. For example, a DHCP server programmed to assign TCP/IP addresses is categorized as a networking server. Similarly, a server handling the routing of data packets through different networks (routing server), is providing a network service and is hence categorized as a network server. Other such services performed by network servers include encryption, decryption, security access, and VPN access services.
- **Internet Servers:** The servers that provide access to common Internet services such as the World Wide Web, Usenet News (NNTP), or even e-mail services based on the Internet, are known as Internet servers.
- **Remote Access Servers:** Such types of servers generally serve as a gateway or access point for users that want to access a network remotely.

An operating system installed on a server is very specific and tailored to enable the performance of the tasks we have just mentioned. For instance, if a server is using an operating system distributed by Microsoft, then it will most likely be using the Windows Server edition. Such operating systems come pre-loaded with networking software. Similarly, a server can also run Linux or UNIX distributions designed for networking. Depending on the operating system installed, a server can either perform the networking functions or be specific to only a few. But it’s not always necessary for a server to comply with every network function; depending on its purpose, a server can only be tasked with a few networking operations, and that will be adequate. In this way, users can deploy multiple servers, each optimized for certain network operations.

Here are a few features that qualify a server for a different class of computers as compared to domestic client computers.

- Server computers natively incorporate the element of redundancy inside their hardware architecture. This means that even if something within the hardware

breaks or fails, the server will still keep running normally. To achieve this redundancy, the internals of a server computer are lined with multiple power supplies and cooling fans, shielding the computer from malfunctioning due to the failure of any corresponding hardware component.

- The subsystems of a server computer are also specifically designed to optimize data flow. If we analyze a typical server, we will see that the design scheme for the disk, memory, and network subsystems are different than those used for a desktop computer. This design supports a high-performance boost to not only the subsystems mentioned above but also to optimize the flow of data. So, data moving to and from different points such as the server, the client, and the network is comparatively more optimized and faster.
- Since servers hold a crucial position within a computer network, special care is taken for the "health" of the computer. Server computers feature specially designed surveillance parameters on both software and hardware levels; the machine itself can keep an eye out for any alarming deterioration in its health and essentially warn the users of imminent failure before it happens. For instance, one of the common monitoring items installed in servers is temperature monitors; if the temperature of the server's surroundings rises too much, it gives off a warning detailing the problem. In this way, the people maintaining the server learn of a problem before it causes hardware failure and can prioritize resolving this issue.

Hubs, Switches, and Routers

The purpose of hardware components such as hubs, switches, and routers is purely to facilitate the establishment and proper functioning of a network. Hence, these three components are 'pure' networking hardware and categorized under the class of 'internetworking devices.' These components are essentially the foundation of any basic or complex network, as the entire cabling

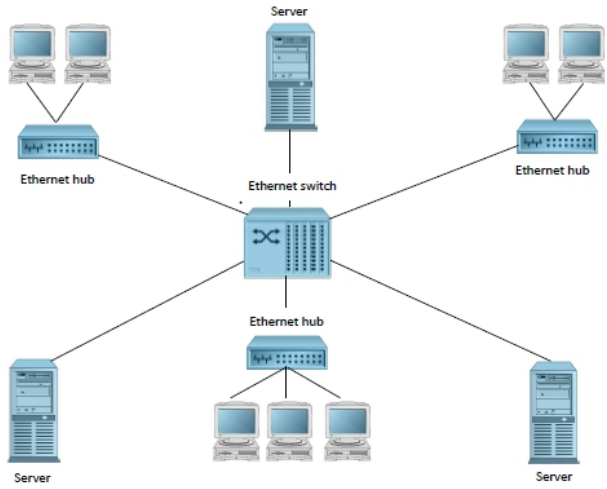
system in a network is connected to these devices. In terms of the OSI networking model, the data flow from these devices can be defined at the physical, data link, or even the network layer.

Let's talk about **hubs** first. Hubs are also commonly called 'concentrators.' The core purpose of a hub provides a point of central connection for the network cables. Hubs can support multiple network cables; the number of cables is a matter of the hub's size. A typical small hub can connect network cables coming from two computers while a large hub can support over sixty computers (depending on the specification). The most popular hub is neither 'small' nor 'large', but a 'medium-sized' hub that generally supports up to 24 client computers.

In a hub, there is a logical wire through which the connected client computers communicate with the network. The capability of this logical wire is known as the 'collision domain.' Sometimes, interference results when too many client computers are connected to a single hub and attempt to communicate with the network.

We will now discuss **switches** . The circuital infrastructure (how the wires have been arranged) of a switch is strikingly similar to that of a hub. A switch also looks similar to a hub. Although the conceptual foundation of the working of hubs and switches are also very similar, the similarity ends there. Unlike the hub, each connection port on a switch has its own collision domain. In this way, each network connection on a switch can freely communicate with the network through a separate collision domain rather than a single one.

Each network connection on a switch is made to be a private connection. Nowadays, most computer networks implement switches instead of hubs, mainly because they are a cheaper solution. However, switches also have numerous benefits over hubs (we'll leave this discussion for some other time since the main focus is to learn how they work). Good network solutions will use one or more backbone switches, which connect to the main switch(es). These backbone switches generally operate at a speed much higher than the main switch(es). However, even if hubs are used in a network solution, there will still be the use of a backbone switch (which is simply an individual switch connected to the hub). The figure below shows a typical arrangement of switches and hubs in a network.



Last but not least, the **router** . By now, we have given adequate attention to the details of how a router works and functions. We now know that the primary job of a router in a computer network is to route the data packets effectively through one network on to the next. A router can also be a bridge that offers a path of flow for the data packets between two connected networks. These two networks establish a connection to the router by using their respective types of wiring and connection.

Let's understand this better through an example. Consider a router in a network that establishes a connection between a 10Base-T network and an ISDN telephone line. In this scenario, the router is dealing with two network connections, one from/to the 10Base-T network and the other from/to the ISDN telephone line. The job of the router will be to create a proper route for the data packets to travel between these two network connections.

Besides these defined network connections, the router can also have another terminal connection. The purpose of this secondary connection would be to program and maintain the router itself.

Cabling and Cable Plants

When setting up a computer network, you'll find there is a huge variety of network cables available to use. But on this level, we

should only concern ourselves with the main network cables commonly used.

The most common network cable used while setting up a Local Area Network connection is the Category 5 twisted-pair cables. These cables are also called ‘Cat-5’ cables. The cable has four twisted pairs; this means it has eight wire contact points. Due to this design, the cable can carry the network signal to each of these eight wire points. The Category 5 twisted-pair network cable is primarily used with Base-T networks such as the 100Base-T network and the 1000Base-T Ethernet network.

A lower-grade version of this same network cable is also available, and it is termed ‘the Category 3 twisted-pair cable’. The overall design and structure of the network cable are similar to that of the higher-end Cat-5 cable; the main difference is the number of pairs it supports. While the Cat-5 cable has four twisted pairs of wires, the Cat-3 cable has two twisted pairs of wires, i.e., half of the Cat-5. Hence, the Cat-3 twisted-pair network cable is generally used to support older network connections such as the 10Base-T network and uses connectors comparatively smaller than the Cat-5 connectors.

Similarly, there are newer and improved versions of the Category 5 twisted-pair cables available now. There is the improved Cat-5E cable and the new Cat-6 standard network cable. There isn’t much difference between the Cat-5 and the newer versions; the Cat-5E and Cat-6 are essentially the same as Cat-5 cables. The only difference is these newer twisted-pair network cables support higher network specifications, making them ideal for installation in networks running at higher speeds. Since there’s little physical difference, the newer versions are backward compatible with the older network types. If you used Cat-5 cable for a 100Base-T network, then you can also the Cat-5E and Cat-6 network cables for the same network connections.

Another type of network cable popular in the past but is not so common for newer network installations nowadays is the **coaxial cable** . This cable can be found installed in old network installations in old buildings.

Let’s talk about the structure of the coaxial cable. In this network cable, there is a central core, usually no more than a thick wire, made up of copper and known as the ‘conductor.’ This core is

surrounded by a plastic material. This plastic cover over the conductor is wrapped with a 'shield' which is basically braided metal. Over this shield, there is an outer covering made out of plastic. Back in the day, you might have seen a thick cable that would connect your television set to the TV cable station's network. This cable was also a type of coaxial cable, and this same cable was also used for cable modems as well in the olden days. The particular coaxial cable used in networks such as 'Thin Ethernet' or 10Base-2 was the RG-58 coaxial cable.

Similarly, for networks such as ARCnet, another (but similar) coaxial cable would be used, which was the RG-56 coaxial cable. The coaxial cable to be used would depend on the specification of the network in which it was being installed. A network's specifications would define the support for a certain type of coaxial cable. This imposed a limitation on compatibility and universal usability of the coaxial cable. This meant that different coaxial cables could not be mixed when setting up a network, and it was very important to use the specified cable for the network being built.

Let's move on to discussing **cable plants** . A 'Cable Plant' is a term used to describe the complete installation of the network cable in the designated building. When we talk about a network's cable plant, we are referring to the network cables, the connectors, the wall plates, the patch panels, and the networking equipment related to networking cables installed in the building. On the surface, the network cable installation and cable management might seem like a simple to-do task, but quite the opposite. Cable plants are very difficult and complex; due to this, it is always recommended to choose a vendor that is adept and experienced in cable plant installation.

Workstation Hardware

In a professional setting, the computers being used by the people connected on a network are network workstations. Generally, the workstations are the network client PCs on a network. However, workstations can also be modified to function as network servers. A workstation termed a 'network client' usually has these features.

1. It is an Intel-based computer
2. It is usually running a Microsoft Windows-based operating system

3. The install Operating System includes NIC and network client software (this enables the network client workstation to communicate with the network)

In the features mentioned above, we said that a network client workstation usually runs a version of Windows as the main OS. But the keyword here is 'usually.' There are cases where network workstations use an operating system other than Windows. Such computers have the hardware and software to allow the workstation to participate on the network even if the operating system is different. For example, Apple's Macintosh and Unix-based computers can also be used as network workstations.

Utilizing the Network Traffic and Knowing the Network Hardware

In the earlier sections of this chapter, we discussed the hardware components involved in every network setup. We also learned about the purpose of each component in a network. In this section, we will go a step further and discuss the actual functionality of the hardware in directing network traffic.

In any network design, the very fundamental and basic approach to test its capability is to see how effectively the network can direct the network traffic from node to node. This test determines if the designed network is good enough or if it is underperforming. To perform this test, the first requirement is to put the network hardware components in a configuration that allows the network to send signals through the connected hardware components efficiently. This is done while keeping the type and connectivity pre-requisites of the network under consideration.

In this section, we will discuss the following basic networking hardware components.

- **Repeaters** : These devices lengthen the traveling distance of the network traffic in the corresponding network type.
- **Hubs** or **Concentrators** : These devices are used when setting up a network with a star topology. Hubs connect the different nodes.
- **Bridges** : These devices are the same as repeaters but more intelligent. Bridges direct network traffic to different segments. This is done so the segmentation is

only performed if the traffic's destination is actually the other segment itself.

- **Routers** : These devices simply route the network traffic effectively and efficiently.
- **Switches** : These devices serve as a quick and efficient point-to-point connection for the other connected network hardware.

Repeaters

A hardware device used in a network to lengthen the range of the network is called a repeater. Repeaters extend the network's reach by boosting the signals. Whenever a network is installed, it is a given there will be places where the network signal is weak. The repeater will take this network's side where the signal is weak, boost this weak signal, and then send it out through the other side. Repeaters are most commonly used for networks with a limited range, such as thin Ethernet networks. Hence you will see the use of repeaters in such network setups. However, this does not mean that using repeaters is limited.

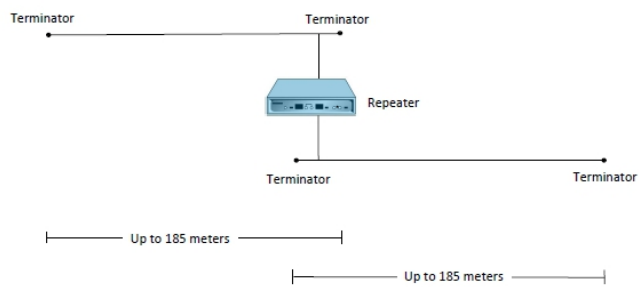
But repeaters can be used for virtually any network connection. For example, consider a typical 100Base-T network installed using Cat-5 network cables. The maximum length of this cable is one hundred meters, meaning that's the range of the network. By using a repeater in this network setup, we can double the range of the network signal to two hundred meters.

In terms of the OSI networking model, operating repeaters is a process in the first layer, i.e., the physical layer. A repeater device is not intelligent. This means that a repeater does not have the hardware capability to understand the signals it is transmitting. Since the only job of the repeater is to perform a network signal amplification it needs to be used carefully. A repeater will not discern between a network signal and an interference signal (usually called "noise"). This is why they should be used only after careful assessment of the network. Otherwise, a repeater might amplify the noise in the network.

Repeaters cannot be used to connect different network mediums. For instance, if a repeater is being used with a 10Base-2 Thin Ethernet network, then it can be connected only with another 10Base-2 Thin Ethernet network.

If we critically analyze the intelligence of a repeater, then we can find it does possess a slight hint of intelligent functionality; nevertheless, this is not enough to perform complex operations such as discerning between the signal types being transmitted. The extent of the intelligent functionality of a repeater device is the ability to separate a connection from the others when the device detects any problem or anomaly in the connected network. For instance, let's consider that we are dealing with two segments of a thin ethernet network. These two segments are connected by a repeater device. If these two segments become broken, then instead of shutting down the entire network, the repeater will still allow the functional segment to keep on working. In this way, the users of the network can access the resources on the network segment still functional but won't have access to the resources on the broken segment. However, one thing to note here is that even if the repeater does separate the working segment from the broken segment, if the main resources such as the servers are on the broken segment, it will be useless. This is because even if the workstations were on the functional segment, they won't be able to access the main networking resources of the server.

The figure shown below depicts a typical repeater setup extending the length of the network.



Hubs (Concentrators)

Hubs are known by these terms:

- Intelligent LAN concentrators
- Concentrators

This hardware device is used in a network setup to connect the nodes to the backbones. If we discuss the topology of the network

where hubs are being used, we can see that the nodes are connected to the hub in a star-like shape. This means that the network cables connected to the hub fan out to each corresponding node. This arrangement of the cables remains the same, whether a hub is being used in a star topology or a ring topology network. In smaller networks, there is no need for backbone switches, and hence, there is no need for a hub. However, hubs can be used in simple networks and large complex networks.

Regarding the compatibility of hubs with the network media types, fortunately, they offer seamless compatibility. This means that a hub can be used with any network without worrying about compatibility issues. If we go further and look at the top shelf higher-end models of hubs, we will see they feature a replaceable module through which a single hub can support multiple network media types. For example, a high-end hub model can support both Ethernet and Token-ring network modules.

Hubs come in many sizes. Some hubs offer support for up to 2 workstations while others for more than a hundred workstations. It all depends on the needs of the network.

Here are a few important characteristics of a hub.

- Just as how a sound from one source echoes in the farther depths of a cave, a hub echoes the data from each of its ports to all the other corresponding ports. Even though the wired arrangement of hubs is star-styled, their logical functioning is more akin to that of bus topology. However, due to the echoing of the data, no logic or filtering process can stop data packet collisions originating from the connected nodes.
- A distinguishing feature of hubs is that they can effectively cut off a misbehaving node from the other properly functioning nodes by shutting it off. This process is also known as ‘partitioning.’ The scenarios in which a hub partitions a node include detection of a network-cable short circuit, an excessive influx of data packets from a hub port flooding the network, and detection of a serious problem relating to the hub port. Effective partitioning of a malfunctioning node prevents the same effects from negatively affecting the other nodes functioning normally.

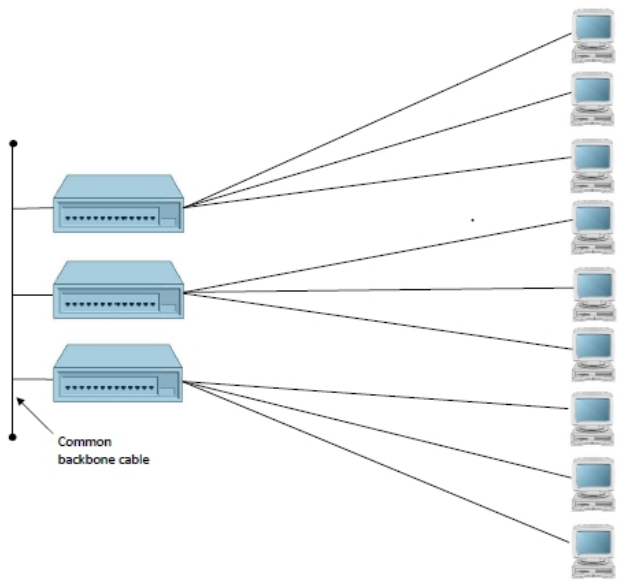
As technology is developing, the mechanics and infrastructure of a hub device are also becoming increasingly sophisticated. Newer versions and models of hubs include pretty neat and advanced features out of the box.

- Hubs now include a built-in management feature; by using network management protocols such as SNMP, a hub can be managed centrally, over the network.
- There are hubs now available that can automatically detect the connection speed of the network and run each node at that speed. For instance, a hub detecting a 10Base-T network will run each node at 10 Mbps. Similarly, for a 100Base-T network, the hub will run each node at 100 Mbps.
- Hubs are using uplinks with faster speeds to connect to a backbone. The average speed of the uplink is usually ten times that of the basic speed of the hub. For instance, a hub with a basic speed of 100 Mbps will have an uplink with a speed of 1 Gbps.
- Hubs now come with a built-in bridging and routing feature. Previously, networks using hubs would require separate dedicated hardware devices to perform bridging and routing functions. With this function built into the hubs, using such devices has become obsolete.
- Hubs feature a built-in switching function. With this feature, the hub can switch the nodes instead of sharing them.

When choosing a suitable hub for your network, the first thing to bear in mind is the specifications of your network. By knowing how many nodes are supposed to be connected to the hub, the required bandwidth for each node, and the network backbone type being used with the hub, we can choose the right hub best suited for the network. In terms of the network backbones usually installed with a hub, they are generally anything between shared 10 Mbps thin ethernet networks to 100 Mbps 100Base-Tx and high-speed networks. Whatever the case, the choosing of a backbone technology primarily depends on the bandwidth requirement of the network and other criteria that need to be fulfilled for the network designed.

Technically, in a network where hubs are being used, the hubs

act as ‘collision domains’, where collisions usually occur. So, if we use multiple hubs in a single network set up, then the area of the collision domain in the network will inevitably become larger. The only exception is when the hubs are individually connected to a switch. By using switches, we can restrict the collision domains of each hub to itself. The figure shown below depicts a network using several hubs.



Switches

Just as the name implies, a switch is a hardware component of a network that can rapidly switch connections from port to port. A switch creates these connections in a network by switching dynamically among the several network ports available. Consider a train yard, where several trains are coming in from certain tracks and leaving through other tracks. The train yard has a designated person tasked to manage the movement and routes of the train. This person is called the ‘yard manager.’ To make sure that the trains arrive at their destination, the yard manager essentially switches the tracks according to their specified route. In this analogy, the ‘switch’ is the ‘yard manager.’ Instead of directing trains by switching the tracks, a switch directs the data packets through the network by ethernet cabling. In this way, a data packet is

effectively routed to its destination.

We know that a switch establishes an individualized connection between any two given ports of the network; it makes sense that the entire ports converging into the switch device don't share a common collision domain. This is why a switch device plays a role somewhat similar to that of a super bridge.

Due to the nature of switches, they are mostly used to bridge the connection between hubs and relatively faster backbones in a network. For instance, consider a network using ten hubs. Each hub supports up to 24 connection nodes for workstations. With ten hubs, we will have about 240 connection nodes meaning there will be 240 workstations in total connected to the hubs. If these hubs are connected to the same backbone in the network, then it would mean that the collision domain of all the hubs would be the same. When the 240 workstations are sharing the same collision domain, then network performance will deteriorate. Here, we can fix this problem by using a switch with 12 ports. Earlier, each port of the switch had its own separate collision domain. Here, all ten of the hubs connected to the 12-port switch will have domains, thereby maintaining the network quality.

A 100Base-T network connection is commonly used with workstations. A networking expert would recommend a 1000Base-T or faster connection as the backbone network. By using a switch and a fast backbone, the workstations connected to the network through the nodes can operate at 100 Mbps.

Switches impact the speed and performance of the network so well that using a switch becomes a no-brainer. Another aspect that makes switches so desirable in networks is that they are very inexpensive. For a typical local area network, using switches instead of hubs makes more sense because hubs are expensive network components. In comparison, a switch is inexpensive, has much to offer to the network, and is comparatively easier and simple to install. Nowadays, you might find difficulty finding an available bridge on the market as the supply and demand of switches is overwhelming.

The reason to know and understand hubs is that although they are not used now, you might still come across older installations using hubs. In newer network installations, it is guaranteed that you will exclusively deal with switches instead. To reiterate the main

concept of these hubs and switches, hubs create a bigger packet collision domain, while switches have smaller, separated collision domains.

Bridges

A bridge is a hardware device that performs the same function as a repeater but is more intelligent. Bridges work by joining two network segments, just like repeaters; the main difference is that when a bridge must pass data traffic from a segment to another segment, it does so intelligently. This means that a bridge will only pass the data traffic to the other segment if this traffic's destination is the target segment; otherwise, it will not. Another distinguishing feature of a bridge is that they also divide the network into smaller segments. Certain bridges can be connected to two network segments. For instance, such a bridge can span from coaxial Thin Ethernet to a twisted-pair Token Ring.

We talked about the layer at which repeaters operate at (which was the physical layer of the OSI model). One would assume that since the function and purpose of the bridges is virtually the same as repeaters, they would also operate at the first layer of the OSI networking model. However, that's not the case; instead, the bridges operate at a layer that is one level higher, i.e., at the second layer, also known as the data-link layer in the OSI networking model. This is because bridges connect the network segments and then pass the data traffic from segment to the other segment 'intelligently.' To do this, the bridge analyzes each encountered data packet's MAC, or Media Access Control address. This analysis of the MAC address helps the bridge determine whether it should forward the data packet onto the other network or not. A bridge device can store the parts of the network's address data. This can be done in either of two ways.

1. The user programs a static routing table that contains the address information and data.
2. The user implements a dynamic learning system that learns in a tree pattern by automatically identifying and discovering the network's addresses.

Bridges shouldn't be used carelessly. Here are scenarios where using bridges in the network is recommended.

- If you are dealing with a small-scale network, then

bridges can be used.

- If the network is using a repeater, then a bridge can be installed in place of the repeater.
- If the network you are dealing with seems to benefit when the network traffic is not transferred unnecessarily between the different segments of a network, then a bridge should be used.

Routers

Continuing the chain of intelligent iterations of the other hardware components of a network, a router is basically a bridge, but even more intelligent, just as a bridge is an intelligent version of a repeater. Just as bridges operate at one layer higher (at the data-link layer) in the OSI networking model than repeaters, routers operate at the third layer of the OSI networking model, also known as the network layer. Routers are more efficient and far better than bridges for transmitting data packets to their respective destinations.

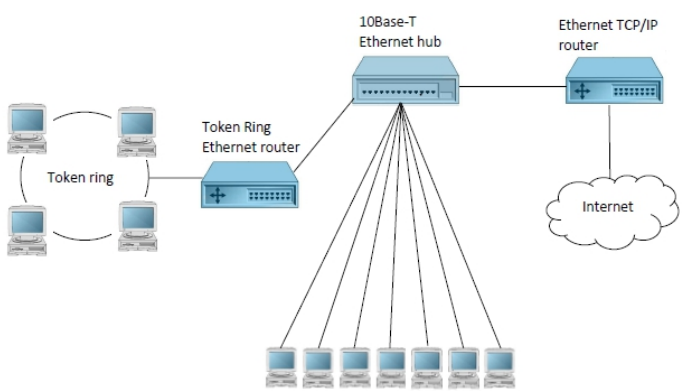
Since the operation of the router is at the third layer of the OSI networking model, the only requirement for the upper layers of the OSI model to establish a connection with the router is that of using the same protocols. If the router is configured and designed specifically for protocol translation, then it can translate any protocol from the first three layers (physical, datalink and network layers) to any other protocol also a part of these three layers. A router can also connect two networks that have no similarity to each other (while connecting similar networks is a given). Generally, routers are best suited and commonly used for Wide Area Networks (WAN) as they can effectively create the links required for this network to be established.

If we analyze the characteristics of the router which allow it to effectively connect two similar or dissimilar networks, we conclude that a router essentially serves the purpose of a node. Routers feature their very own network address, which solidifies their function as a node even more. A router receives data packets from other nodes. After receiving the packets, the router analyzes and examines the contents of the data packets: only after this assessment does the router send the data packet to its destination. This procedure needs to be performed almost instantaneously to

avoid delay and lag in data traffic. To ensure that the router swiftly and accurately performs this job, they are designed with a microprocessor inside them to handle the computational and logical needs of the task. Usually, this processor is a variant of the RISC or Reduced Instruction Set Computer type chip. Besides a microprocessor, routers also have built-in memory to help with routing function. Since routers are more intelligent than bridges and they have more computational resources; they can figure out the shortest route (if available) towards any data packet's destination and use it.

Besides this, routers can also perform certain tasks that facilitate the bandwidth maximization of a network. Also, a router can logically and dynamically adapt to the traffic problems detected in a network.

Let's talk about the importance of routers in a network. It wouldn't be an exaggeration to say that routers form the backbone of the entire Internet. For instance, consider the TRACERT command. When you use this command to trace a route from two points, a node to a destination, we can see there are multiple 'hops' shown by the terminal before it can show the destination. These 'hops' are routers that are forwarding the data packet until it reaches its destination.



Routers are not pre-configured. To perform their tasks and functions properly, they need to be programmed. For instance, a standard router configuration may include the assignment of network addresses to each of its ports and the configuration of the protocol settings. The programming of routers is usually done in

either of these two ways.

1. Usually, there is a port known as the 'RS-232C' port. By using terminal emulation software, we can connect a computer or a terminal using this port. Once connected, it becomes possible to program the router in text mode.
2. Besides programming a router directly from its RS-232C port, routers can also be programmed by using network-based software that comes with it. Usually, this software uses either a graphical tool or a simple web interface.

Both of these two methods are supported by the majority of the routers available nowadays. However, there is no recommended method. It all depends on aspects such as your security needs and the specific model of the router you are using. When using routers, one should be careful, as the network-based programming method for a router can be exploited by hackers. This would allow unauthorized users to change the configuration of the router.

Gateways

A gateway is an application-specific interface. The main job of a gateway is to link all layers of the OSI networking model whenever they are detected to be dissimilar. This dissimilarity can be in any single layer or all layers and the gateway will still perform its function. To understand this better, let's see an example. Let's say we have established networks by using the OSI networking model, but we want to connect to a network using Systems Network Architecture, also known as SNA, by IBM. These two networks are not similar, so to connect them, we will use a gateway to do so. Gateways also can translate Ethernet to Token Ring. However, there are simpler network solutions if you need a network translation such as this one. Since the translation load on gateways is considerably larger than other solutions, gateways perform relatively slower.

Nowadays, using gateways in networking is primarily to handle e-mails. For example, two of the most common e-mail protocols handled by gateways are:

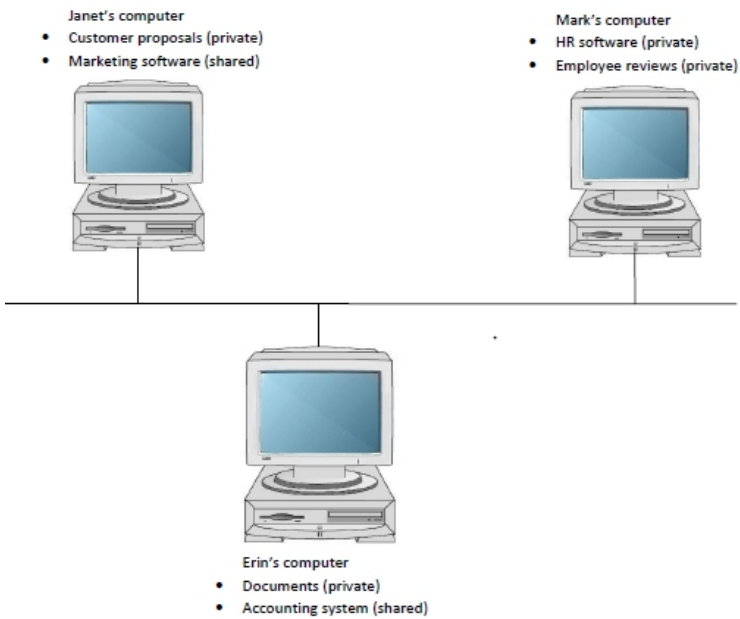
- POP3
- SMTP

Generally, the majority of the e-mail systems that need to

connect with systems on a different network will either use a computer set up as a gateway or use the e-mail server to perform the gateway tasks.

The Core Fundamentals of Cable Topologies

Before we move on to the cable topologies, let's refresh the concept of a 'Topology.' The word 'Topology' means 'shape'; similarly, the word 'Network Topology' essentially refers to a network's shape (the wired arrangement of the network's nodes).



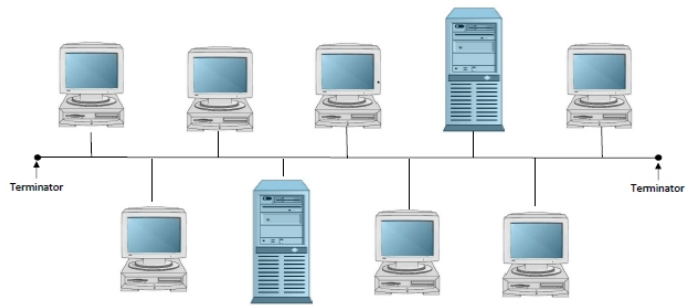
Different topologies have different costs, advantages, disadvantages, performance, stability, and reliability. In this section, we will discuss the three main cable topologies commonly used today.

1. Bus Topology
2. Star Topology
3. Ring Topology

Bus Topology

Bus topology is also commonly called 'Common bus multipoint topology.' A bus topology is basically a network that uses a single

end-to-end network cable. On this network cable, some devices are connected at different locations on the cable, and these connections are termed ‘nodes.’ A simple illustration of a bus topology network is shown below:



However, there is no universal bus topology in use. Instead, bus topology comes in many types, each featuring its own specifications. These specifications are based on these factors:

- The number of nodes that can be handled by a single segment
- By using a repeater, what is the resulting number of segments that can be used
- The maximum limit of physical proximity for the nodes
- The network segment’s length
- The coaxial cable required
- How the segment’s terminal ends are supposed to be terminated

Generally, a bus topology network implements coaxial cable. In such a type of network, the two open terminal ends of the network need to be addressed; otherwise, the network would not be functional. A special type of cable terminator is used on each terminal end of the network.

There are several different bus topology, and each group uses a different type of connector to conjoin the different segments of the network cable. For instance, a Thin Ethernet 10Base-2 bus topology network uses a connector known as a ‘BNC connector.’ This

connector is also known as the 'BNC-T connector' because it resembles a 'T' shape. This connector allows a node (computer or a server) to be connected to the network segment while allowing the network to continue its bus. There are also different types of BNC connectors:

1. BNC-T connector
2. BNC barrel connector
3. RG-58 cable with male BNC connector

In terms of budget, the bus topology network is the least expensive option of the three. This is because a bus topology network uses comparatively less network cable regarding the star and ring topology. Hence, a bus topology network uses less networking materials and needs less installation labor. However, while the bus topology has advantages over the other two topologies with cost, it also has significant drawbacks.

A network with a bus topology is more sensitive and prone to failure because it comprises multiple subscales, which essentially create a segment. These subscales must be connected to the nodes. Now, this level of intricacy introduces a new problem, and that is:

- If the segments of the bus topology network fail, it will cause the failure of the segments in the network.
- Identifying the source of failure is even more tedious and time-consuming, as the technician must go through the available cable connections until the source of the defective segment is identified.

Since a bus topology network is seemingly unreliable and more prone to failure, many new wired network installations do not use this topology. However, bus topology networks may be seen in older network installations.

The most commonly used bus topology network used back in the day and still in limited existence today is the 10Base-2 Ethernet network (also known as Thin Ethernet). A Thin Ethernet network has these characteristics:

- 10 Mbps maximum speed rating
- Type of network cable and connectors used are '**RG-58/AU** ' or '**RG-58/CU** ' (coaxial cable and BNC connectors respectively)
- To function properly, the network requires each

ending of every segment to be terminated with a 50-ohm terminating connector
- Maximum node capacity per segment is 30 nodes
- Maximum segment length is 185 meters, or 607 feet
- Repeaters can feature extended segments
- The minimum distance between each node should be 0.5 meters or 1.5 feet of cable distance.

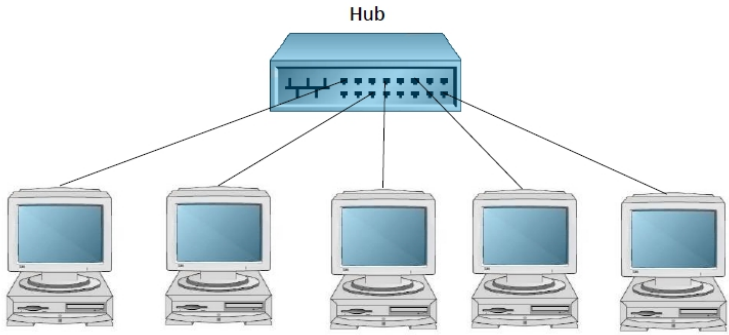
In a network using bus topology, with repeaters enabling the user to connect up to three segments together, each connected segment would support up to 30 nodes (counting the repeater as a node). Two more segments could be added, if the sole purpose was extended signal distance and they had no nodes connected to them. This would make five segments that could be added by using a repeater. The maximum length of the entire repeated segment should not exceed 925 meters, or 3,035 feet. To remember this arrangement, we can simply remember the 5-4-3 rule:

- Five segments
- Four repeaters
- Three populated segments

Star Topology

In a star topology network, the connected computers, servers, or simply nodes are hooked up to a single central unit. In this wired arrangement, the connections radiate out from the main unit, similar to the shape of a star. This central unit is commonly called a ‘hub’ or ‘concentrator.’ The hub hosts a bunch of network cables that radiate out to the corresponding nodes on the network. In technical terms, a hub is known as a ‘Multistation Access Unit’ or simply ‘MAU.’ However, this term is strictly used with Token Ring networks.

In a star topology network, there are multiple hub size options available. For instance, some hubs can support no more than two nodes, while there are also hubs that can support up to ninety-six nodes. Generally, a standard central hub unit used in this network has support for up to 24 nodes. Regardless, even if we use a 24-node hub or a 96-node hub, we are still given the freedom of connecting multiple nodes into a hub and shaping the network as we see fit. Here’s a simple illustration of a star topology network.



However, remember that, since a hub is used as the central unit, there come complications in the previous sections of this chapter. A hub echoes the network traffic among its other ports. So, the network traffic from any node will be echoed to the other nodes. This means that a node's entire bandwidth connection is shared among the other node connections. For instance, if the total bandwidth speed of the hub is 100 Mbps, but one nod is using only 50 Mbps of that total bandwidth, then the other nodes cannot access the rest of the bandwidth and instead, must share this 50 Mbps. To put it into simpler terms, the total bandwidth available to one node is the same bandwidth shared among the other nodes.

In a star topology network, there are multiple Ethernet connections available for use listed below.

- **100Base-T Ethernet** is the most commonly used and provides a bandwidth limit of up to 100 Mbps.
- **10Base-T Ethernet** is seen in older networks. This ethernet has a bandwidth limit of up to 10 Mbps
- **1000Base-T Ethernet** is a relatively newer Ethernet standard and is commonly known as Gigabit Ethernet. It offers a bandwidth capacity of 1000 Mbps or 1 Gbps.
- **10GBase-X** is the most recent Ethernet standard. It is called 10 Gigabit Ethernet and uses a fiber optic cable connection offering a bandwidth capacity of 10 Gbps.

Let's talk about the cable requirements of the 10Base-T and 100Base-T Ethernet network connections.

- 10Base-T Ethernet requires a Category 3 (Cat-3) twisted-pair network cable.

- 100Base-T Ethernet requires a Category 5 (Cat-5) twisted-pair network cable.

Remember that although 10Base-T Ethernet can use a Cat-5 network cable, 100Base-T Ethernet cannot use Cat-3 network cables. Whenever installing a 10Base-T Ethernet or newer network connections, it is recommended to use the latest networking cables. For instance, if you are using a 10Base-T Ethernet connection, then you can use a Cat-5E, and if money is not a problem, then you can even go for the Cat-6 network cable.

Here are wiring characteristics that 10Base-T networks share.

- They require four wires in two single-sheathed twisted pairs. These twisted pair wires can either be shielded or unshielded.
- They can function on Cat-3 network cables and newer ones such as Cat-5.
- There is a length limit for each node connection of 100 meters, or roughly 328 feet.
- They are not bound by a limitation on the number of nodes per logical segment.
- For all of their connections, they use 'RJ-45' connectors.

A notable advantage that 1000Base-T networks have over 100Base-T networks is that they:

- Are compatible with Cat-5 network cables
- Operate at ten times the speed of 100Base-T networks, i.e., at 1 Gbps or 1000 Mbps as opposed to 100 Mbps

Arguably one of the most important advantages that 1000Base-T networks have is their Cat-5 cable compatibility. Nowadays, the most commonly used network cable in over 75% of the installed networks is none other than Cat-5 cables. If a Cat-5 cable system is already present, a 1000Base-T network can be installed without changing the cable system. This provides a huge saving in not only time but in installation costs, cabling costs, and labor costs, since installing a new cable networking standard for a whole building is very expensive.

Here are a few characteristics of 1000Base-T over Cat-5

networks.

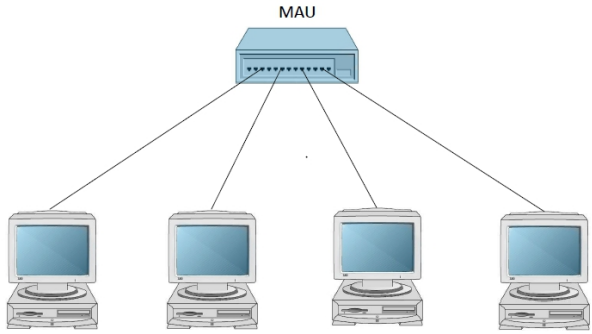
- These networks need eight wires in four single-sheathed twisted pairs.
- They require at least Cat-5 or better network cable standards (Cat-5E or Cat-6).
- The length limit for each node connection is 100 meters or roughly 328 feet.
- They are not bound by a limitation on the number of nodes per logical segment.
- For all of their connections, they use 'RJ-45' connectors.

You will see that 1000Base-T networks are strikingly similar to their predecessor 100Base-T networks except in areas such as network cabling requirements.

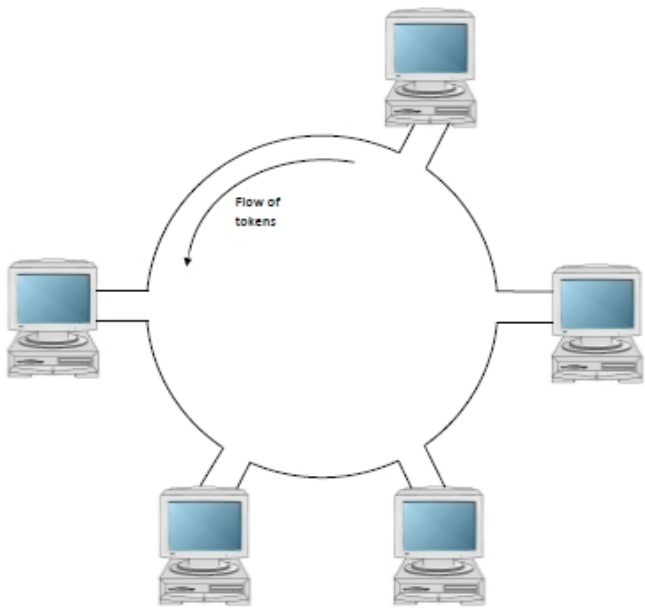
Star topology networks are more expensive than bus topology networks because the use of wired network cables is greater. Also, the labor costs to install that wire is more expensive, and the need for routers or hubs also stacks up the overall cost. However, this expensive budget is not worthless. Star topologies are more reliable and offer better performance than networks using a bus topology. Not only does it offer higher bandwidth performance, if the isolated network connections break or go bad, but the other connections will remain unaffected. Even if a problem does come up in a star topology network, it is easy and simple to troubleshoot as each network cable is going from the hub to the node directly.

Ring Topology

Unlike the other two topologies we have discussed so far, that use an arrangement of physical network cables, a ring topology network uses a logical arrangement instead. To elaborate, in a ring topology the actual physical network cable arrangement is that of a star topology, and each node of the cable is connected to their very own Media Access Units. But here's the catch; despite the physical arrangement, the network cables electrically behave as a ring. This means that the signals coming from the network travel through the different nodes in a ring. A simple illustration of a ring topology network is shown below.



(Physical Representation of Ring Topology)



(Electrical Representation of a Ring Topology)

Unlike the bus and star network topologies based on Ethernet, the ring topology is based on Token Rings instead. Sometimes, a network using a ring topology can also be seen running on a fiber-optic network, usually with a bandwidth capacity of 100 Mbps instead of copper-based cables. This network is based on FDDI or Fiber Distributed Data Interface. The main use of a ring topology is for big telecommunication networks such as the Synchronous Optical Network, which is also known as SONET. Ring topology is

also used in storage area networks.

Chapter 4: Wireless Communication Systems and Connecting to the Internet

What is Wireless Communication?

Wireless communication rarely requires a physical medium or a channel to transmit the signals. Rather these allow the signals to travel through space and are commonly called an unguided medium of communication.

Connecting to the Internet

In this section, you will learn about the fundamentals of Internet connectivity and its features.

Wide Area Networks

Wide Area Networks or WAN is just a Local Area Network with a wider range. Wide Area Networks can be defined as multiple interconnected Local Area Networks. WANs are preferred when a better and wider range approach is required of a Local Area Network. Establishing Wide Area Networks can be done in multiple ways. To determine which method to adopt in setting up a WAN, the organization or company need to consider different aspects such as

- The regularity with which the Local Area Networks must be used.
- The regularity with which the Local Area Networks must be connected with each other.
- The “bandwidth”, or data capacity required by the network.
- The measurement of the distance between each Local Area Network point.

By factoring in these aspects, a suitable solution can be implemented to establish an optimal Wide Area Network. For instance:

1. Establishing a Wide Area Network using a leased telephone line capable of supporting a bandwidth of up

to 56Kbps.

2. Establishing a Wide Area Network using dedicated DS1 lines capable of supporting a bandwidth of up to 1.544 Mbps.
3. Establishing a Wide Area Network using dedicated DS3 lines capable of supporting a bandwidth of up to 44.736 Mbps.

A Wide Area Network can even be established by using a private satellite, which ultimately supports even higher bandwidth. Hence, to choose the best option for a WAN connection, it is recommended first to assess the situation and needs to come to a clear solution.

The emergence of Wide Area Networks began when users on a Local Area Network needed to access the resources on another Local Area Network. This was all too often observed in big institutions such as business companies, organizations, hospitals, banks, and schools, etc.

Let's discuss a brief example. Consider a big company with several buildings specializing in their respective functions. There's the main headquarters of the company, and then there are the warehouse units of the same company but in a different location. Now, the main headquarters of the company houses some much-needed resources such as the ERP, or Enterprise Resource Planning system. For the warehouse to properly perform its job, it needs access to the inventory and shipping functions provided by this resource. Since the warehouse and the headquarters are in different physical locations, the Local Area Network of the warehouse needs access to the Local Area Network of the headquarter. So, the company will implement a Wide Area Network connection to resolve this issue.

Generally, if an organization can design the infrastructure of its system so it does not need a Wide Area Network connection, this is better. The reason for this lies in the cost required to maintain the Wide Area Network links properly.

Internet and Intranet

Remembering the wide-spread popularity of the Internet and its importance in our modern society, the productivity of any business company is crippled if they do not properly use the Internet. Handling and maintaining Internet connectivity on a network is a

very pivotal job, as even several minutes of Internet downtime can create a pile of problems for the organization. Hence, the Internet is a very crucial service and feature of computer networking. Now, very few people are unfamiliar with the Internet. With its amazing productivity and reachability, virtually all companies today take advantage of the Internet's key services such as e-mails, accessing the World Wide Web, and using the Usenet newsgroups.

Implementing an Internet connection on a network involves another entity known as the Internet Service Provider (ISP). The connection of a person or organization with the ISP is basically a telecommunications network connection. The connection from the ISP to the client is established by using a physical medium such as a line. There are several types of connections offered by ISPs depending on the client, for example

- DSL line
- ISDN line
- Fractional/Full DS1 connection

After a suitable line supported by the ISP is chosen, it is installed into the designated domicile by stretching the line to the building and connecting it to a special box, which is known as a CSU/DSU (channel service unit and data service unit). The main purpose of this box is data conversion, i.e., converting the form of data being carried by the specified local telephone company into a form usable by the Local Area Network. Also, this CSU/DSU box is then connected to a router (or a modem), which handles the routing of data packets between the Local Area Network and the Internet. Sometimes, this CSU/DSU box is built within the router provided by the ISP.

Now let's discuss the security of an Internet connection. When an ISP "ships" an Internet connection to its client, they provide them with a router during the installation. The data packets being sent out by this router are automatically filtered to prevent a data packet leak.

The more common software-based security generally adopted by users is a 'firewall.' This program is what intelligently limits any unnecessary connection to a server on the Internet that an application on the computer might request. It also blocks harmful incoming traffic, which is usually from a hacker. So, by using a firewall, we can secure our computer systems from potential online

threats while using the Internet.

So far, we have discussed the Internet as an immensely interconnected network of people around the world. We will now discuss something similar to the Internet, and that is the 'Intranet.' They sound and work similarly.

While the Internet is basically focused on external connectivity, an intranet is a form of network focused on internal connectivity. For instance, let's say there is a company that wants to host a web page or even a server only for its employees to access. It needs an Intranet. The company will use a primary web server that will store all the resources of the company, such as documents, employee handbooks, invoices, and all such data regularly published within the company for the employees and departments. Hence, it becomes a miniaturized version of the Internet solely dedicated to the internal network infrastructure of the organization. However, the functionality of the intranet does not simply end here. It can perform Internet-related tasks, such as providing File Transfer Protocol (FTP) and Usenet servers.

An intranet is implemented and maintained by the organization or company within the limits of its own Local Area Network. Usually, an intranet is not accessible from outside the LAN, but there are cases where penetration can happen.

Understanding the Features of Networking

Up to now, we have discussed the simple relationship between computers connected on a network (P2P and Client-Server Networks). Now that the reader has developed an understanding of how connected computers interact with each other, we can discuss some tasks that they can perform on a network. This can be called the features of computer networking. In this section we will discuss these features:

- File Sharing
- Printer Sharing
- Application Services
- E-mail
- Remote Access

File Sharing

Back in the day, file sharing was the very reason that people would

use computer networks. In the mid-1980s the ability to share files and data from one computer to the other connected in a network without using physical storage devices was a revolutionary deal. Although it may not seem like much today, consider this: to share a file or media content with your acquaintance, you first had to store it in removable media storage and then physically get that media to that person. File sharing was so important that companies would specifically install a computer network to use this feature.

File sharing usually entails the files that people would need to access regularly. Spreadsheets and word processing files are common examples, although there are many others. To enable file sharing, the first requirement is for those computers that require shared access to be connected in a network. Next, there should be a 'shared drive' which acts as a network place for the files to be stored while allowing users connected to the same network to access these shared files on their system remotely. To eliminate a repercussion of file sharing, namely that any user can modify the contents of the shared file, the system should have proper authorization privileges in place. This means that not every user in a computer network will have administrator rights that will allow them to change the files or the shared drive. This is also known as 'file locking.' Another reason for file locking is so the multiple users who are accessing the shared drive or the folder are not modifying it with conflicting changes simultaneously.

Printer Sharing

The printer sharing feature is also of great importance and makes computer networking even more useful. As the name suggests, printer sharing refers to sharing the printing resources between users within a computer network. If a company places a printer in one office, then it is possible to share the functionality of this single printer with every employee in the office using a computer network. This is not only economical for the company but the users. Since the office requires only one printer, the company can afford to pitch in for some high-quality top of the line printer designed to handle huge workloads. By implementing a computer network, a company can enjoy the economic benefits of printer sharing.

Now we'll discuss some details of how printer sharing works. Even though there are multiple ways printer sharing can be done, the most common method is to use a printing queue that holds the

printing requests of the users in the interconnected computer network. This queue ensures that the printing task in progress is not disturbed by the other incoming printing requests, and the new printing tasks are not performed by the machine until the current task is completed. This method is recommended due to its efficiency.

Another way of performing printer sharing is to allow the independent workstations to have direct access to the printer itself. The printer itself supports a setting where it's configured to connect to a network as an ordinary workstation would. If there is a high demand for the resources of the shared printer, then the independent workstations are instructed to stand-by until it’s their respective turn. But this is not efficient.

In the printer queue method, there is a special server known as the ‘print server’ which automates sending print requests according to their timestamps or urgency. There are several ways to set up a print server.

1. Using a file server connected to the printer network.
2. Using a workstation running special printing software and is connected to the network and printer. In this way, the software communicates with the other computers on the network, taking their print requests and forwarding them to the printer through the host computer.

Application Services

This feature is similar to the two features we have recently explored, i.e., file sharing and printer sharing. The application service feature allows users connected on a network to share applications. For instance, if a company invests in a licensed software to be used by its employees, then it can take advantage of computer networking to generate shared copies of the application on to the network server to be used by others. The working of this feature is very simple; a workstation connected to a network can access the shared application, load the files from the shared drive into its system memory, and run the program.

By using this feature, the organization can also save on effective storage on its workstations, as every user would access a centralized folder on a server to run a program instead of installing the same

program individually on each running workstation.

Another way to use this feature is to establish a shared installation point on a network server. This allows the users who wish to install the application to access the installation setup directly from the network instead of downloading it or using physical media storage such as CDs, DVDs, etc. Hence, the user can directly copy the contents of the installation setup for the program onto their respective workstations and install the program as usual.

E-mail

It wouldn't be an exaggeration to regard e-mail as one of the most resourceful, convenient, and efficient ways of communication that have ever emerged. The e-mail feature observes a widespread use in different environments, be it a local or professional setting. On the outside, e-mail seems very simple with a sender and receiver. Although this covers the gist of it, we will explore the e-mail feature in more technical terms.

Generally, there are two types of e-mail systems. One is a file-based e-mail system, while the other is a client-server-based e-mail system. The one most people are readily familiar with is the client-server-based e-mail system, but we will come to that later. First, we will discuss how a file-based e-mail system works.

A file-based e-mail system is simply made up of a server and a controlling host known as a ‘gateway server.’ The server defines a storage location that consists of shared files. The server is to provide authorized users access to these files. However, handling the connection requests between the server and an external user falls under the jurisdiction of the ‘gateway server,’ which is actually a single computer. This computer runs a special software known as ‘gateway software’ to handle this job, and the unity of the server and gateway server is what makes up a file-based e-mail system.

But a client-server-based e-mail system is something cleaner, sleeker, more powerful, and, most important, secure. This e-mail system also boasts extended functionality; for instance, in business companies, they can automate the e-mail system for generating invoices and making purchases automatically. It’s a given that such an e-mail system must be properly configured to do so. The client-server-based e-mail system consists of a single server responsible for collectively managing the external and internal e-mail interconnections on the network. This e-mail system also houses the

messages. Some examples of a client-server-based e-mail system are Microsoft Exchange and Lotus Notes.

Until now, we have mainly discussed these two e-mail systems in large-scale business companies. However, the e-mail feature is equally important for small-scale companies and organizations, such as those with less than twenty-five employees. For such companies, purchasing an entire e-mail system and maintaining it is comparatively expensive and requires much manpower for proper maintenance, hence making the use of e-mail systems out of their reach. However, there is another viable alternative for such scenarios. This includes using an e-mail system not primarily housed and maintained within the organization itself. For instance:

- Set up a shared connection with the Internet so every employee using a workstation can access it. Next, we have to do only simply set up the corresponding e-mail accounts for the users either through the ISP or just use an e-mail service free and popular such as Yahoo!, Hotmail, Gmail, etc.
- Use the 'Microsoft Windows Small Business Server 2008' as the dedicated Operating System for all the workstations. This OS includes useful server-based tools that can facilitate setting up an e-mail system. Best of all, the OS is natively bundled with a limited version of the 'Exchange Server' software that can be used.
- Subscribe to a mailbox from a service provider that has set up and maintained an e-mail system with high specifications. Companies that go for this approach usually have just to pay a monthly fee that corresponds to the number of mailboxes being used by them.

Remote Access

Another beneficial feature of computer networking is giving users the ability to remotely access the resources of their specific network. The reason that makes this feature so important is that a network's physical limitations are ignored by the users, meaning they don't need to be in the office or the building where the network is located. They can remotely access their files or e-mails even when they're working away from the office, such as in their

homes or a hotel. However, remote access is not a simple feature. But remote access can be delivered in a variety of flavors. To set up and use the remote access feature, the list shown below outlines several methods that can serve the purpose.

- Using the Microsoft Windows Server operating system to establish a RAS (Remote Access Service) connection. This connection entails a simple setup consisting of only one modem to an enlarged system that involves multiple modems.
- Using a remote access system set up and maintained to perform only this function. Such a system can handle multiple simultaneous connections at once, meaning that several computers can be set up easily. Each computer that is connected to the remote access system uses its own network card.
- Setting up a workstation with specific remote access software (for example, pcAnywhere and GoToMyPC) through which the users that intend to use the remote access feature simply dial in.
- Establishing a company connection to the Internet. The employees of this company can use this Internet connection to gain access to the resources available on the company's networking system. To secure this remote access, the company usually implements a Virtual Private Network connection (VPN).
- Using a workstation running the Windows Server operating system as a connection server. This can be done by installing software such as Windows Terminal Services. In this way, the workstation will be capable of hosting several client sessions allowing multiple users to gain remote access.

Chapter 5: Common Network Protocols and Ports

Unlike the previous chapter, which covered more than half the topics under the scope of this book, we will be briefly going over and understanding some of the most common protocols we come across in networks. Network protocols are complex and difficult. We will reserve the more intricate details for the next series of this book and focus instead on the fundamentals of network protocols to build a basic conceptual foundation.

In this chapter, we will be mainly discussing:

- TCP/IP and UDP Ports
- Other network protocols such as DNS, DHCP, HTTP, FTP, etc.

TCP/IP and UDP

TCP and IP are two protocols used in harmony with each other. The explanation of each protocol is:

1. **TCP:** Also known as the 'Transmission Control Protocol.' TCP operates at the transport layer of the OSI model, and it mainly manages the connection between the computers on a network. The messages of the TCP protocol are 'encapsulated' in IP datagrams.
2. **IP:** Also known as the 'Internet Protocol.' IP operates at the third layer of the OSI networking model, i.e., the network layer. The main function of this protocol is to define the way network data is supposed to be addressed from its source to destination, respectively. IP also defines the sequence in which the data is supposed to be reassembled when it reaches its destination.

UDP is known as 'User Datagram Protocol,' and it basically has the same job as TCP/IP protocols, with the only catch being that it offers limited features as compared to its counterparts. Although the UDP protocol is also carried by the IP datagrams, it has only a reliability feature, and that is that the UDP protocol will resend the

data packets that did not arrive at the destination.

The only advantage UDP has over TCP/IP is that it is considerably faster. However, it offers little error-checking and correction capability. Hence, UDP is best suited for trivial network communication tasks. Since UDP does not check for errors and simply resends the data when any error does come up, it should be only used for network communication when the reliability features are not important or if the application involved in the network communication offers its own extensive error handling and checking.

The other networking protocols have been explained in chapter 2. Recall that they are:

Domain Name System (DNS), allowing users to access websites with easy-to-remember domain names instead of long numerical IP addresses.

Dynamic Host Configuration Protocol (DHCP), for assigning TCP/IP addresses to the nodes in a network.

Hypertext Transfer Protocol (HTTP), which controls the transfer of data between the client and the webserver.

File Transfer Protocol (FTP), which defines the method by which file data is sent and received between the FTP client and the FTP server.

Network News Transfer Protocol (NNTP), specifically used for Usenet discussion groups on the Internet.

Simple Mail Transfer Protocol (SMTP), which handles the sending and receiving of e-mails from one e-mail server to another.

Chapter 6: Learning About the OSI Networking Model

The very important, fundamental key to understanding computer networking is to perceive the conceptual realms of the OSI networking model. This is where all the beginners in IT start. The OSI model defines most methods along with the protocols through which computers connect and communicate with each other on a network. When understanding the OSI networking model, the reader must firmly grasp the abstract visualizations as this will help create a strong foundation for network designing and network solution engineering.

The OSI model is an accurate yet fundamental portrait of how networking in the real world actually works. Although there are subtle differences between the theories and practical implementation of the networking, it is by no means something that one should disregard.

By understanding the OSI model, we are essentially learning about the intricacies of computer networking, and the reader can eventually visualize the networking process of computers. And this understanding is the key to success in the practical field of networking. The basis of a certified networking professional is to have an adept and comprehensive understanding of the OSI networking model itself.

We have discussed the importance of the OSI model enough, now let’s talk about what it’s all about. As the name suggests, the OSI Networking Model is simply a framework that defines the operations and workings of modern networks. The model is divided into seven distinct and separate layers. Each layer possesses a trait known as ‘successive dependence.’ This means that the successively higher layers in the model depend largely on the services characteristic of the preceding lower layers.

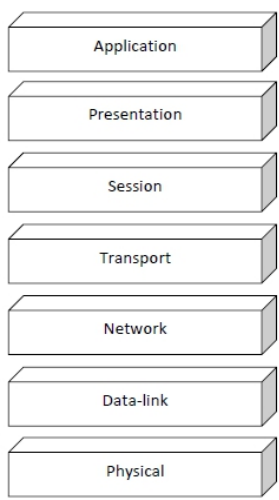
To understand this better, let's use an analogy. Think of a standard desktop computer system you would commonly find in your home. Now, this computer's several components work together, which makes the computer itself functional. If we divided this computer into layers such as in the OSI networking model, then

according to this standard, the hardware component of this computer will be termed as the 'lowest layer.' The layer succeeding the 'hardware layer' of this computer would be the Operating System along with the respective system drivers. It's a no-brainer that the Operating System and the respective drivers would be useless without the corresponding hardware. Hence, this higher layer is depending on the preceding lower layer to perform its function properly. Similarly, this successive hierarchy extends to the point where an application is displaying useful and digestible data to the user.

The seven layers of the OSI Networking Model are:

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

The figure shown below depicts the structure of the OSI networking model in its basic form.



(Physical – Layer 1 up to Application – Layer 7 – in the OSI Networking Model)

Layer 1: The Physical Layer

The first layer of the OSI networking model is the physical layer.

This layer essentially defines the characteristics of the physical parts used in a typical network connection. For instance, in a network connection, the physical layer specifies the network cable, the router, the DSI/CSU box, and the other physical mediums involved.

The network cable transmits the data packet stream (in bits) from one node to the other in the physical network. Let's discuss this physical connection in a little more detail. The network connection established through this cable can be in either of the two forms.

- " Point-to-Point", a network connection established between two points.
- "Multipoint", a network connection established between several points, for example, a single point connecting to multiple other points.

The direction of transmission is also an important point of discussion in networking. This direction dictates the order of transmission, i.e., a data packet can be transmitted from one side of the network in one direction at a time. The sender transmits data received by the target, and only then can the receiver transmit data packets back to the sender. Hence data transmission is happening in opposing directions in turns). Similarly, in another type of data transmission on the network, both the sender and receiver can send and receive data simultaneously (data transmission is happening in both directions simultaneously). These two types of data transmission are called:

1. **Half-Duplex** : data can be transmitted only in one direction at a time.
2. **Full-Duplex** ; data can be sent and received in both directions simultaneously.

The physical layer also specifies the method of bits transmission in the specified network. Transmission of bits in a network connection can be done in either of the two ways, i.e., **Series** or **Parallel** . Generally, the majority of network connections transmit bits serially, but the OSI networking model also accounts for the parallel transmission of bits.

To further clarify the physical layer's specification, here's a small list of metrics that generally fall into the category of this layer.

- The network cable being used

- The voltage being carried by the cable
- The measure of the electrical signal timing
- The distance through which optimal data transmission is supported by the network cable

Layer 2: Data-Link Layer

The second layer of the OSI networking model is the data link layer. This layer defines those standards which give a sense of comprehension and value to the data packets or bits being transmitted and received by the physical layer. The data link layer of the OSI model bridges the connection between the third layer (network layer) and the first layer (physical layer) by defining and implementing a reliable protocol through which the network layer transmits its data through the physical layer.

The main purpose of the data link layer in the OSI model (besides linking the first and third layers) is to perform a data proofreading function. This is an informal and easy to understand way of describing the data-link layer's secondary job. According to technical standards, the data link layer performs detection and correction of errors within the outgoing data streams. In this way, the network ensures a reliable and error-free stream of data. Also, the data link layer features a term known as 'frames' that refers to the data elements that are carried by this layer. There are multiple frames, and some of the most commonly used ones are:

- X.25
- 802.x (includes Ethernet and Token Ring networks)

In the OSI networking model, the data link layer is further divided into two sub-layers. These two sub-layers are:

1. **Logical Link Control** (LLC)
2. **Media Access Control** (MAC)

Now, these two sub-layers collectively perform the main function of the data-link layer. This means that each of these two sub-layers individually performs separate tasks associated with the functionality of the data-link layer itself.

The LLC sub-layer establishes a link and controls it, i.e., call setup and termination along with transferring data. Due to this, the OSI model is compatible with networks such as telecommunication

and LAN.

The MAC or Media Access Control sub-layer handles the assembly and disassembly of frames in the network, with addressing as well as error detection and correction. Now you can see these functions as the distinguishing characteristics of the data link layer itself.

Here is a list of some of the most common MAC protocols in the second layer of the OSI networking model.

1. 802.3 Ethernet protocol
2. 802.5 Token Ring protocol
3. 802.12 100Base-VBG protocol
4. 802.11 Wireless protocol
5. 802.7 Broadband protocol

Out of all these MAC protocols, the Ethernet and Token Ring protocols are the most common in computer networking.

Layer 3: Network Layer

The third layer of the OSI networking model is the Network Layer. This is the layer where most of the crucial networking functions are performed.

There are several functions involved in this layer, but we will only discuss the major aspects which have a significant impact on the working of a network. Generally, the Network Layer determines the path or the route by which the data packet will travel from one node (point) to the destination point (node) on another network. The main job of the network layer is to define the route through which the data packets will travel from network to network.

Regarding the protocols used in the network layer, there are several, but the most important of them are the

- Internet Protocol (IP)
- Internet Protocol Exchange (IPX)

These protocols contain information which specifies the source and destination routing for the data packets. Hence, each network packet using these protocols can tell the network its destination based on the routing information from the protocol. After the data packet reaches its destination, this protocol also helps the receiving computer identify the source from where the data packet came.

The Network Layer holds significant importance in the OSI model

for defining the transmitting of data packets from a single or multi-router setup. Before we discuss more details about these layers, let's also clarify the job of the router devices. A router is simply a piece of hardware designed to

- Examine each data packet
- Transmit the data packets to their intended destination by analyzing the source and destination address information

The Internet is a complex network, and a data packet being transmitted over the Internet might need to pass through several routers before it can arrive at its destination. But on a comparatively simpler and smaller network, the data packet might need to go through only a handful of routers or none.

When analyzing the network layer in a little more depth, an interesting point becomes clear. If the Network Layer is separated from the first (Physical) and the second (Data Link) layers, we realize that the protocols of this layer can function independently of these two lower layers. To put it into simpler terms, we can use the protocols of this layer in any variation and effectively use it with the lower layers without having to establish a chain of independence. For example, if the computers share a commonality regarding the first two layers, then the IP protocol and the IPX protocols can establish a network between these two computers. If we take this concept and apply it to a real-world scenario, then it would mean that a data packet using the IP protocol can be transmitted over an Ethernet, Token Ring, or even a wired cable connecting the computers. The same holds true for data packets using the IPX protocol, with the pre-requisite because the computers both support the IPX protocol and share a commonality in terms of the lower-level layers. In such a scenario, a network connection can be established.

Layer 4: Transport Layer

The major concern of the transport layer is mediating the movement of data between the different layers. For this purpose, the transport layer masks the characteristics of lower layers from the upper layers in the OSI model. Besides this, the major functions of the transport layer include:

- **Flow Control:** directing the transmission of data

between the sending device and the receiving device mainly to manage the influx of data that the receiving device experiences. The transport layer ensures that the receiving device is not flooded with more data than it can process.

- **Multiplexing:** divides a physical channel into multiple logical channels, which makes it feasible for multiple devices or applications to transmit data over one physical channel (or link).
- **Virtual Circuit Management:** Managing virtual circuits in a network in the sense of establishing, maintaining, and terminating the said virtual circuits.
- **Error Checking and Recovery:** incorporating the applications of multiple mechanisms to achieve the function of identifying data transmission errors and trying to rectify this error, for instance, issuing a request to the transmitting device to re-send or retransmit the data.

If we talk about the core purpose and functionality of the transport layer, then it would be essentially to handle the information flow that streams from one node to another node in a network.

Like the rest of the layers we have discussed up till now, the transport layer differs from them in the sense that for each operating system, implementing the transport layer is done differently.

The Transport Layer features a bunch of important protocols. Out of these protocols, the following two are used in connection with either IP or IPX data packets, respectively.

1. Transmission Control Protocol (TCP); used with the Internet Protocol (IP)
2. Sequenced Package Exchange (SPX); used with the Internet Protocol Exchange (IPX)

Layer 5: Session Layer

The fifth layer of the OSI networking model is the Session Layer. By this layer, the model can define the connection established between two computers, either in a client-server connection or a peer-t0-peer

connection relationship. The term ‘session’ is used to describe this virtual network connection between computers. Since the primary focus of the OSI model’s fifth layer is upon these connections, hence it is named as the ‘Session Layer.’ the reason the establishment of a network connection between two computers is known as a ‘session’ is that once the connection is established, it persists for a certain period.

A session basically involves negotiations that take place between the connected client and the host. The points of focus in the negotiation are listed below.

- Flow control
- Transaction processing
- User information transfer
- Network authentication

Layer 6: Presentation Layer

One of the higher tier layers, the presentation layer, is mainly concerned with presenting data in a form that can be comprehended by the system. The presentation layer of the OSI networking model collects all the data being supplied by the lower-tier layers. It then converts into a format that can be used by the system. Even though the name ‘Presentation’ may be misleading, the deliverance of data to be easily understood by the system is as important as the system presenting the data to be easily understood by the user.

The presentation layer performs these functions:

1. Data compression
2. Data decompression
3. Data encryption
4. Data decryption

From this, we can conclude that the main concern of the presentation layer is *data* .

Layer 7: Application Layer

The last and highest tier layer in the OSI networking model is the Application Layer. If we analyze the nature of the interaction of each layer with their respective elements in a network, we can see a steady pattern. The layers in the OSI networking model begin their

interaction with the physical elements within a network, i.e., the routers, network cables, etc. From here, the layers move toward interacting with virtual features and elements, i.e., moving toward intelligent aspects of the network. After this, the OSI model's focus on the virtual aspects of the network shift towards the involvement of the computer machine itself within the network, which is evident from the last two layers (Presentation and Application layers).

Continuing this train of thought, we can come to understand the purpose of the application layer in the OSI networking model and the overall working of a network involving computers. By doing this, we can analyze networks in a more detailed and comprehensive manner.

Now let's get to what the application layer is all about. The main concern of the application layer is to control and mediate the interaction of the network with the Operating System and the applications installed on this OS. It defines how the applications handle the communication that the system becomes involved in when connected to a network.

Examples of the software that fall under the definition of the application layer include:

- Windows Client for Microsoft Networks
- Windows Client for Novell Networks

Such software is typically used as a network client application in computer networks.

However, the data does not go through the OSI networking model in only one direction. It can go up the OSI model when the computer is at the receiving end of the network, and the data can go down the OSI model when the computer is transmitting the data through the network.

Chapter 7: Network Security, Cybersecurity, and Hacking Methods

This chapter focuses on the basics of network security and recovery.

Does network security play a vital role?

Internal security makes it possible for a person to protect their network from internal threats, which are more common than external threats.

A network's security is threatened by internal users in these ways:

- By accessing records of payroll and accounting, business development data, and other such information in illegal or inappropriate ways.
- Gaining access to another user's file which should have been inaccessible to others.
- Impersonating another user by sending e-mails under their name to cause mischief.
- Gaining entry into the systems and performing criminal activities that include embezzling funds.
- Letting viruses into the system, by accident or deliberately.
- Discovering user accounts and their passwords helped by sniffing packets.

Such internal threats must be eliminated by diligent management of the network's security. Among the many internal users in the network, at least some have the ability to exploit security holes in the network, and a few of these users might even try to do so.

Account Security

In Account security, various tasks are carried out to manage the user accounts enabled on the network. To make sure that no security holes exist, a person besides the one managing the accounts should audit them often.

Management of the general account security requires these steps:

- The startup user account termed as 'Guest' in most

network operating systems should be removed from the network immediately. Accounts used for testing, such as 'Test', 'Generic', etc., should not be created because these accounts are easy and frequent targets of crackers.

- The network operating system assigns a default name to the administrative account. It may be named as Administrator in Windows systems and Supervisor/ Admin in NetWare. Change this name soon so attacks directed against the account can be avoided.
- Knowing how to remove access to network resources with quick precision from any user account and verify the network resources that contain their security systems. For instance, network operating systems and specific applications like the database servers or accounting systems handle the management of user accounts. Some systems don't deny access to deactivated or removed accounts unless they log out from the system, which can threaten security. It is necessary to discover how the system manages removed accounts.
- Establishing a relationship of mutual trust and working closely with the appropriate people in the Human Resources (HR) department is essential in maintaining proper security. By co-operating with the HR staff, you could work on the security issues related to the departure of employees and make a checklist for standard employment changes affecting IT. The HR department may not provide you with advance notices, but you must know about the terminations immediately for taking proper steps in time.
- Try to provide the new users with a program where they can submit their assigned permissions and have them reviewed and signed off by their supervisor. This step eliminates any possibility of these users gaining access to sensitive information.

Password Security

Password security is an important aspect of account

security, which enables you to set policies that control the time period within which the system forces the user to change their passwords, the complexity and length of these passwords, and whether old passwords can be reused. Password security policies should at least include these suggestions:

- Make sure that the users change their main network passwords every ninety to one hundred and eighty days through the network password policy settings. Even though thirty days is recommended, it can be considered too frequent for some environments.
- 'Reuse policy' should prevent users from reusing an old password for at least a year.
- Make a requirement that the passwords should be at least eight characters long. If the password being set is case-insensitive and does not allow special characters to be used, the possible variations of such a password are almost 36^8 (three trillion). For case-sensitive passwords, the possibilities increase up to 62^8 (218 trillion). If special characters such as space, comma, asterisk, period, etc. may be used in passwords, the possible variations increase even further.
- The users should be encouraged to use passwords that do not make up a word in any language or insert numbers and other nonalphanumeric characters between the letters of the word. In this way, a dictionary attack initiated by password-cracking programs will fail. Mixed-case characters should be used wherever the network supports mixed-case passwords.
- Policies that observe and detect numerous incorrect password attempts should be turned on. This policy is often termed *Intruder detection.* It monitors whether too many incorrect attempts at entering the password have occurred in a set amount of time and prevents further attempts by locking out the account. The locked account can only be reopened by talking to the administrator with the authority to reset the account. This case usually occurs when people forget their passwords, but this policy keeps in check any malicious

intent to guess the password and gain access to the account.

- Novell NetWare and Windows servers can set limits on the amount of time a user can be logged in to the network, and restrict certain users to particular network computers. To impose these limits on every user would be too excessive; nonetheless, it is essential to restrict the administrative account to the fewest possible number of different workstations so a person operating at a different workstation cannot access the account even if they know the password.

According to the Catch-22 of network security policies, making the policies too strict can actually reduce network security. For instance, if the password security policies require the user to use a 12-character password, change it once a week, and prohibit the reuse of passwords, most users cannot remember the changing passwords. They will write it down somewhere in the office, with the risk of it being discovered. To strengthen the security of the network, a balance must be maintained between security and usability.

File and Directory Permissions

Internal security also involves the maintenance and control of users' access to files and directories. The settings related to this security are more difficult than managing the user accounts because every network user has at minimum 20 directories and hundreds of files, and managing this amount is a tough job. To make this task easier, the key is to follow regular procedures and periodically spot-audit particular parts of the directory tree that contain sensitive information. By effectively structuring the overall network directories, the top levels can simply be assigned permissions, which will "flow down" automatically to subdirectories and make identification of the users who have access to specific directories easier.

The settings related to assigning permissions on files and directories is considerably flexible in network

operating systems. Various kinds of roles can be enabled for different users through built-in permissions. The roles mentioned below describe the authoritative ability of what the user can do in the directory:

- **Create Only:** This role gives the user the ability to create and add new files to the directory and prevents the user from accessing, altering, or deleting previously existing files, including those which they created. Helped by this role, the users gain permission to include new information in a directory to which they shouldn't have access otherwise. This role makes the directory function like a mailbox where one can only put new things in it, and only one other person will have full access to the content inside.
- **Read Only:** This feature allows users to see the files at a glance in the directory, and they can view these files on their computer. The read-only role only allows these users to view and read the information in the files, making no kind of changes. Such files can be copied via the read privilege by the users into another location or directory, which allows them to make desirable changes.
- **Change:** This feature gives the user a free hand with the files in the directory, which are inaccessible to other users.
- **Full control:** This role is limited to the owner of a directory who can make any alteration to the directory files and also can grant access to any other user as desired.

On different network operating systems, these features are designed in different ways.

Security for specific files can also be set in a way similar to setting permission for directories. The permissions assigned in both files and directories have similar workings. A user's ability to read, alter, or delete a file can be controlled for specific files, and Directory permissions are usually overridden by file permissions. This concept can be understood by considering a user has access to change the files in the directory. Still, once

the permission is set to read-only for the files in that directory, the user can now only access the read-only feature.

Practices and User Education

The people using the network are part of the reason for insecurity and internal threats. To make sure that the network remains secure and protected despite the threats, it is essential to develop effective security practices and habits.

Besides developing and implementing a good security practice or scheme, it is also imperative to manage it regularly by archiving the procedures related to security and establishing a process to ensure they are followed by the employees daily. A simple and comprehensible procedure easily followed is much better than the poorly followed complex yet excellent procedure. Therefore, the overall design of network security must be made simple while keeping it consistent with the company's needs.

Make it possible for all the users to follow prudent procedures. These procedures can be enforced by customizing the settings available on the network operating system, but formal education of the employees regarding the importance of internal security is also needed.

- Inform the users of the basic conditions they need to follow related to network security and provide them with a document containing the details of network security and the users' role in preserving it. The guidelines in the document for the user could be to choose a secure password and not disclose it, to take care not to leave their network-connected computers unattended for a long time, and to not install software from anywhere else other than the company.
- Discuss the network security issues with the newly appointed employees that will be using the network.
- Examine the company culture, and depending on that, consider making the users sign a form that acknowledges their comprehension of the security procedures they must follow.
- Auditing users' actions related to security should be done at certain intervals, and if some have full-control access to the directory, then keep a check on how they

assign permissions to other users.

- Review the security logs on the network operating system occasionally, and if a problem occurs, investigate it properly.

Network security procedures are designed and implemented while keeping the worst-case scenario in view. Still, most of the time, security issues occur due to an innocent mistake or ignorance instead of malicious intent.

Understanding External Threats

External security deals with protecting the network system from external threats. Before the Internet came into use, the procedures related to external security were easy to manage because the networks used only external modems to connect to the network. But Internet connectivity spread throughout the system increases the importance of external security and also the difficulty in managing it.

As long as the network is connected to the Internet, it can never be secure. Techniques that the crackers develop to overcome the security of a network are implemented via the Internet. The external threats faced by a network develop so rapidly that, if a book were written on all the current threats to a network, it would be out of date when it was printed.

The three basic external security threats are:

- **Front-door threats:** If an external person logs onto the network by guessing or cracking the password of one of the internal users, threats to system security arise termed as front-door threats. The intruder may have succeeded due to having a connection with the company or a personal relationship with someone using the network.
- **Back-door threats:** Back-door threats will arise if there are bugs in the software or hardware of the network operating system. The crackers take advantage of these bugs and breach the network security through them, then continue to find their way to the administrative account and finally taking control of the system. These threats can also be caused if the bugs are purposely programmed into the software of the system.

- **Denial of service (DDoS):** The DDoS attack can deny service to the entire network. A few examples include causing servers to crash by specific actions and increasing Internet traffic by useless data such as flood ping requests.

To counter the problem of crackers, several steps can be taken. These may not fend off the determined and highly skilled crackers completely, but they can make most of the crackers give up.

Front-Door Threats

The most common threat is the front-door threats, where the external person gains access to a user account on the network. Some forms of front-door threats include a displeased ex-employee who had access to the network in time, or an outsider who guessed or cracked the password to a valid user account on the network or got it from the original user of that account.

The current or terminated internal users are more threatening to security because they have certain advantages of knowledge as compared to the regular crackers. They already know the crucial information required for cracking, such as the important usernames to target, other users' passwords during the time they were working together, the network structure, and server names.

Remembering this, internal and external security are interconnected, so if the policies and practices related to internal security are used, front-door threats are greatly reduced.

If the network resources that can be accessed from the LAN are kept separate from those that must never be accessed from outside the LAN, the risk of front-door threats greatly decreases. With providing the external user access to the accounting server, it is possible to manipulate the settings so the system cannot be accessed from outside the LAN.

Network resources can be separated and categorized based on the authorization to access these resources.

- Access to LAN from the outside should be controlled and given only to a specific type of people who need it among the traveling or home-based users. These users access the LAN remotely through the Internet when you run the VPN software for them.
- If the users need to access the LAN remotely,

consider creating remote access accounts for them besides their normal user accounts and set them to be more restrictive than the normal LAN accounts. This method is not generally practical, but the strategy used in it can prove helpful, especially for the users with broad LAN security clearances in normal times.

- The dial-back feature should be used for users that dial into the modems from a fixed location (such as their homes). In this feature, the phone number of the users' system from which they will dial in is securely documented. To connect to the modem, they will dial the system and request access. The remote access system ends the connection and dials the recorded phone number of that user. The user's computer picks up the call and establishes a real connection. In this way, the dial-back feature prevents access to the system if the dial-in phone number differs from the one recorded.
- Once the users with broad access to the system leave the company or are terminated, examine the user accounts to pinpoint the ones whose passwords are known by the ex-employee. After the employees leave, consider changing the passwords of such accounts immediately.

The people who had no kind of association with the company will often try an indirect method termed *social engineering*. According to this technique, they make use of a nontechnological method to gather information inside the company, including user accounts and passwords. Social engineering is most effective in large companies where the employees rarely know each other. One type of method is when a user receives a call from the outsider posing as the network administrator and is requested to give their password temporarily so a certain problem can be tracked down. Another method of the social engineering technique is by searching the trash documents and records for information that may help the culprit to crack a password. To avoid such threats, the employees should be specially instructed to deal with them and to be prudent about giving information over the phone as IT people usually never ask for anyone's password.

Back-Door Threats

Problems and bugs existing in the network operating system or some other part of the network infrastructure (such as routers) are the main cause of back-door threats. Security holes are one problem that persists in all network operating systems and components. It may be effectively dealt with by staying updated with the software and security-related patches as they are released, and reviewing new information related to the security holes that may exist in the software.

Web servers should be made secure in these ways:

- If you host the website associated with your company on an Internet Service Provider's (ISP's) system instead of your network, the server becomes more secure. The external server's good points include increased availability to the server (by providing services 24/7) and advanced security. Another point is that the concern related to allowing or disallowing LAN connections to the network from the outside is no longer relevant.
- Ensure that a strong firewall router is configured and implemented for the system network. The firewall router you set up will be better off being tested by someone familiar with the workings of that firewall or who has helped with the configuration. Keep the software of the firewall updated.
- Investigate the security settings related to the web server being used and confirm that they are properly implemented. By auditing these security settings periodically, the web server and the network remain secure.
- For the people accessing the web server from outside the company, create a web server that can be accessed from outside the firewall, or more precisely from between the firewall and the Internet router (demilitarized zone). This security method creates an obstacle for the crackers that invaded the webserver and will give them a hard time if they try to breach the network.
- E-mails are the most dangerous form of

communication because they might be infected by viruses and Trojan horse programs. If the e-mail traffic is not monitored carefully, these might infiltrate the company network. This threat is prevented by using a virus-scanning software on the e-mail server and updating the virus signatures regularly.

DDoS Threats

Another type of threat to the system network is the DDoS (Distributed Denial of Service) threat by which legitimate users of the network cannot obtain the network resources because they are denied access. It works in two ways, one of which is by flooding the network with useless traffic so the server (such as an e-mail server) denies services to the legitimate users or simply crashes under the heavy traffic load. The other way requires taking advantage of the existing bugs in the software of the network to crash the server.

Prevention of DDoS threats include:

- Checking and confirming if the network's software is updated and current.
- Firewall settings that allow the user to disable the Internet Control Message Protocol (ICMP) traffic service so traffic such as ping requests will not be allowed into the network.
- Not letting the people outside the LAN access those network resources and servers which they should not access. For example, the accounting system of a company is made inaccessible to those outside the LAN because they do not need it. So, the firewall or packet-filtering router is configured so the traffic coming from and going outside the server's IP address is denied.

Potential Attacks and Threats

A wide variety of malicious software exists in the computer world, and the list continues to grow. Some are listed below.

- **Viruses:** A computer virus is a code or program capable of copying itself and spreading by infecting numerous files such as COM, EXE, AND DLL program and application files. The document files for applications like

Microsoft Word and Excel prone to virus attacks support macro languages, which are sophisticated enough to allow it. The data files, such as JPEG image files, are also at risk of being attacked by these viruses.

- **Worms:** The worm program functions by sending a copy of itself to other computers, which spread it to different computers after running it. The e-mail systems have lately been a victim of worms attached to e-mails in an enticing message. If the e-mail user opens the attachment, copies of the worm are spread to other people present in the user's e-mail address book. This action is carried out without the knowledge of the user, and the receivers of the worm face the same situation. In this way, worms spread like wildfire across the Internet through the e-mail server in just a few hours.
- **Trojan horses:** Trojan horse is a deceptive program that pretends to do something meaningful or of interest to the user but carries out malicious activities in the background during the period the user is busy interacting with the main program.
- **Logic bombs:** Logic bombs are malicious programming code pieces added into the normal program by the original author or by a person involved in developing the source code. They are set to become active after a certain amount of time, after which they delete key files and perform other malicious actions.

With each passing day, the already enormous number of viruses increases even more as new viruses are written and discovered. An important requirement of network administration is to establish practices to deal with these viruses.

Antivirus software runs on a network computer and monitors the software activities to search for potential virus threats. If a virus entity is discovered by the antivirus software, it protects the network by removing the virus from the original file while keeping it intact, and quarantines or locks it until an administrator checks it.

Antivirus is developed so it can run on most network computers, including desktop computers, file servers, e-mail servers, print servers, and computerized firewalls. Three most notable vendors among many that provide the services of antivirus are Symantec

(Norton Antivirus), Trend Micro (PC-cillin), and Network Associates (McAfee VirusScan).

The most suitable option is to assure that the Antivirus is running on all the servers and customize the settings so its software is updated automatically.

As e-mail servers are more at risk of virus attacks, it is highly recommended to make sure that Antivirus software is running on them. The newly created viruses associated with e-mails can spread throughout the world in a matter of hours, so if you set the update of virus signatures to be on an hourly basis, you will likely get a necessary virus update before it attacks your network.

Running the Antivirus is also recommended on the workstations but depending only on this software to prevent virus attacks is not the right move. It should not be considered a primary way of dealing with viruses, but as a supplement to the server-based software.

Basics to Hacking and Network Design

In this section, we will be discussing network designing and the basics of hacking. Network designing is a very important job best handled by network professionals. Designing a network from the ground up is time-consuming, stressful, and a very sensitive job. However, in return for carrying such a burden and responsibility, the resulting network built for the company is specifically tailored to their needs. This allows the company to work and function efficiently while using a network. Although network designing might seem intimidating at first, the process and philosophy behind it are actually simple and straight-forward once you get the hang of it.

Last but not least, we will lay the foundation for simple hacking by using the Linux operating system and briefly talk about the kill chain process of hacking that includes reconnaissance, exploitation, and such. However, clarify that covering even the basics of hacking is outside the scope of this book. Instead, we will focus on the major aspects.

The Process of Designing a Network

Network design does not follow a scientific procedure, nor is it an exact science. That’s why getting everything correct on the first attempt to design a network is virtually impossible, as every

network has its own specific needs and demands that need to be met. Prominence and excellence in this task come from experience and practice. However, the trick to designing a good network is to estimate the needs of the network and then try to meet these needs to the best of your ability in the network design.

The network design process is not universal. It varies from person to person. Some processes are simple and easy, and some processes are horrendously complicated. In this chapter, we will learn about a network designing process moderately comprehensive yet very simple. There are only two steps to this process:

1. Assessing the network needs
2. Meeting the network needs

Assessing Network Needs

Assessing the demands of the network is what will set up for good network design. Before we can even consider the specifics of the network design, such as the network cables, the topology, the operating system, etc., we must first understand the goal the network is supposed to accomplish. In the network design process, assessing the needs of the network should be given equal or more emphasis as the other steps.

Here are four questions that can give more than enough information needed in this step of the process:

- How much storage space do we need?
- How much bandwidth capacity do we need?
- What are the network services required in this setup?
- What's the maximum budget for the network installation?

After answering these questions, you will get the majority of the network demands. These sections provide a guideline on how to approach the network design process by assessing the network's needs.

Applications

A productive approach towards assessing the network needs is to understand the applications supposed to be run on the network. The productivity of the network in helping its users defines a good network, and designing such a network is directly related to

accurately estimating its usefulness. Most users on the network will be using software applications. Hence it is very important to make sure that the network supports these applications.

In networks, some applications are common among the different departments of a company, and some applications are specific to a certain department or a certain user. Here's a list of some applications commonly installed for all the users in a network.

- A Word processor
- A spreadsheet program
- End-user database
- A graphical presentation program
- E-mail application
- Anti-virus software

After listing the applications installed for every user, the person designing the network needs to determine how these applications will be used, and how often they will be accessed. For instance, a company of over 1,000 employees will likely have over 90% of its populace using a word processor. Now you just estimate the number of documents created by each user per month, the average size of the document, and the average storage time for each document (usually either dating to 2 years or indefinite). By making these educated guesses, we can estimate the demand of the users from the network based on the average size of the documents created by the users if they wish to transfer such documents over the network. You repeat this process of estimation for the other applications. By doing this, you will end up with a safe guess of what's the storage and bandwidth capacity required for the network.

Once we are done with the common applications, we move on to the department and user-specific applications. For new companies, this step is relatively hard. The person designing the network will be ambiguous about the applications used by the departments unless they are informed about it. Similarly, for companies around for a while, the network designer will already know these specific applications that the network must support. It is very important to know about the impact of each departmental application as it can have a considerable impact on the network. For instance, a department related to accounting will most likely revolve around shared database files. The network design for such a system must

differ from the standard client-server design.

Here is a list of some of the most common categories of departmental applications.

- Accounting
- Distribution and Inventory control
- MRP or Material Requirement Planning
- IT
- Electronic commerce
- Human resources
- Payroll and stock administration
- Publishing
- Marketing
- Legal

Assessing these specific categories of applications is the same as the common applications.

Users

Once we are done with estimating the application that the network must support, we can now work toward assessing the number of users that the network must also support along with the applications used by each user. Assessing the total is relatively easier. The company itself can provide this information, or you can infer it from their business plans and the long-range budget.

While designing a network, one should also factor in the growth capacity of the company, i.e., the network should be capable of supporting new users that join the company in the coming years. By studying the growth rate of the company, this demand can also be factored in while designing the network.

Besides estimating the number of users that will be on the network, we also need to factor in some important questions about the users, which have been listed below.

- **The Bandwidth Requirement:** Aside from the normal use of network services, does any user have significant bandwidth requirements?
- **Storage Requirement:** Are there any users with significant storage requirements besides the general requirement of the majority of the users? For example, if the electronic imaging department needs to catalog many documents into an image file format on the

network's server, then how many users will need to access this cataloged data?

- **Service Requirement:** Are there any users in the company that need access to additional network services that most users normally do not? This question can be related to a group in a company that deals with sensitive data and needs to be partitioned from the rest of the groups on the local area network by using a network firewall.

Network Services

While designing the network, consider the range of network services. For different companies, the requirement for network services is also different. For instance, if a company requires a simple network setup, then it might only need simple network services such as file and print services along with an Internet connectivity service. But a complex network setup will include many other network services. Here's a list of the network services that should be considered when designing a network for the company.

- File and print services
- Backup & restore services
- Internet connectivity
- FTP & telnet
- Web browsing and external e-mail services
- Internet security
- Remote access services
- DHCP services
- Centralized anti-virus services
- WAN services to other places
- Streaming services
- VoIP

There are three main aspects you must know for each of the network services.

1. The storage and bandwidth needed by each service.
2. Knowing the way these services will be provided to the users. Knowing the server that will host these services. Each server needs to be set up.

3. The network service requirement of the users or groups in the company. The company will not require every network service to be available for the users. Other times, there will be users or groups within the company that will need access to specific network services as opposed to the general populace of the company.

Meeting the Network Needs

Once we are done with the assessment of the network requirements, the next thing to do is ensure these requirements are met. This step of the network designing process basically depends on the experience and resourcefulness of the person in charge of designing. There is no defined series of steps that, when followed, will give us a definite answer in what to do. Instead, you need to map the entire network to paint a portrait of what the network will be like. The foundation of this portrait will be the knowledge you have gained up to now in the assessment step of the network designing process. Another good practice is to seek feedback on your network design from networking professionals that have loads of experience in this field. Gathering advice from different critics and implementing it in your design may be the recipe for successful network design.

The Basics of Hacking: The Kill Chain Process

The main focus of hacking is usually penetrating a network or a user account. The latter is simpler as several techniques can be used to approach hacking someone's account, such as using a brute force attack. In this book, we will discuss hacking regarding penetrating a network. However, we cannot cover every aspect related to hacking because an entire book can be written on this topic alone. Hence, we will only go through the main process of hacking, i.e., the Cybersecurity kill-chain process.

A Cybersecurity kill chain process has eight essential steps, and these are:

1. Reconnaissance
2. Intrusion
3. Exploitation
4. Privilege Escalation
5. Lateral Movement

6. Obfuscation
7. Denial of Service
8. Exfiltration

These eight steps are the very core and fundamental stages of a penetration attack by a hacker. No matter what type of attack you want to launch on a network, whether it be an internal attack or an external attack, you must follow through these eight phases to succeed in hacking.

Phase 1: Reconnaissance

The first phase of the kill chain process is to gather information about the target. In this stage, the hacker's job is to simply observe the target and research information about the target through online resources. The attacker can look around the social media pages of the company it wants to target or go around gathering information about the company's employees from their social networking accounts. In modern days, researching a target is relatively easy, with so many resources at the hacker's disposal. An attacker determines the internal situation of the company itself by keenly observing it from an outsider's perspective. This reveals the potential weak links within the company's network that the attacker should target. During reconnaissance, hackers usually take either of two approaches:

- Passive Reconnaissance
- Active Reconnaissance

In passive reconnaissance, the attacker does not directly risk exposing his attempts to the target. Instead, he aims to gather as much information about the target as is available to the public and then to create links to other potential targets. For example, garnering an employee's name from the company's website, then looking up his social media accounts from his name, then figuring out his username, and the chain of investigation continues. The information gathered is publicly available, and this raises no alarms.

But in Active Reconnaissance, the attacker takes a more aggressive approach towards gathering information about the target. When following this approach, the attacker usually engages with the target system directly to figure out the potential vulnerabilities. However, doing so carries a certain amount of risk

because the attacker's information-gathering attempts can be discovered by the target, and the attacker can then be exposed. Once the attacker has gathered information such as the names, titles, e-mail addresses of the target, the reconnaissance phase is complete, and he can now explore the different avenues through which he can proceed with the penetration attack.

Phase 2: Intrusion

Once the attacker has gathered the information, he can devise a way that will give him access to the target's system. The focus of the attacker in this phase is to somehow get into the target's system by taking advantage of malware or security vulnerabilities. Once the hacker is inside the target's system, he can set up for the later stages of the kill chain process. After this, the information gathered from the reconnaissance phase will help the hacker to devise a believable and feasible attack, such as a spear-phishing attack. By sending a carefully constructed e-mail with a compelling context, an attacker can easily trick the target into clicking on a malicious link. This will give the attacker access into the target system and even more control of the system, i.e., by injecting spyware to gather passwords and other such information from the background without the target realizing. This phase of the kill-chain process is basically the entry-point of a penetration attack.

Phase 3: Exploitation

In this phase of the penetration attack, the attacker infects the system with his own malicious code. This exploitation of the target system will essentially provide the hacker with better control over the target system. Exploitation needs to be done carefully. First, the target should not know the fact somebody has sneaked into his system. The exploitation phase mainly focuses on giving the attacker more resources to work with on the target system by exploiting the vulnerabilities discovered in the reconnaissance phase. An attacker can also install tools, create scripts, or even perform modifications to the security certificates of the target's system.

Phase 4: Privilege Escalation

Sometimes, the target the attacker exploits has lower user privileges by default, or the attacker is only given lower privileges by the operating system after penetration. In such cases, it is of

paramount importance for the attacker to elevate his access privileges in the target system. Otherwise, he will be locked out of most of the system's resources even after successfully penetrating it. In an analogy, privilege can be described in the following way. The attacker has successfully penetrated a building undetected and is now in the lobby; however, unless he escalates his privileges, he will stay stuck in the lobby, and that's practically useless for his objectives. Some of the most common approaches for escalating privileges are:

- **Brute force attacks** - this approach targets the password vulnerabilities to give the user administrator credentials, which can then access the system as an administrator rather than a standard user.
- **Exploiting zero-day vulnerabilities** - zero-day vulnerabilities are those weaknesses in the security of a system or framework present from day one of its development. The special thing about such a vulnerability is that neither the user nor the developer knows this potential flaw making the exploit attack virtually unstoppable.

Phase 5: Lateral Movement

Now that the attacker has complete control of the system's resources, time to find the jackpot he came looking for. In this phase, the attacker will move from one system to the next in search of more data and assets. This phase is a sort of data discovery mission for the attacker. The goal is to find sensitive and critical data.

Phase 6: Obfuscation

In this phase of the process, the attackers conceal their presence and cover their tracks. This will prevent immediate discovery of the attack and also make the future investigation of this attack more difficult. In this phase, the hackers usually delete metadata files, overwrite the timestamps, and make other such modifications.

Phase 7: Denial of Service

In this phase, the hackers target the network and its corresponding infrastructure by temporarily dismantling it. In this way, normal users won't be able to access the network and won't know what's going in their systems and network. This is also

commonly known as a DDoS attack.

Phase 8: Exfiltration

This phase of the kill-chain process is the escape route of the hacker after he has gathered the data and information he came for. The main focus here is to somehow move the data from the target system to a system specified by the hacker, either by copying, moving, or transferring the data over the network. This process can take time, but once the data is out, the hacker can do anything he wants with it.

Chapter 8: Useful Cybersecurity Tips for 2020

Vital Function of a Disaster Recovery Plan

A disaster recovery plan is a document containing the step-by-step procedure of recovering a network after a disaster endangers the network data or hinders its functioning. The external financial auditors of a company need the annual disaster recovery plan to get the information listing the network data and its significance to the company, and repair the detrimental effects a network failure can have on the company network. While preparing a disaster recovery plan, the manager must carefully consider all the possible disaster scenarios and develop effective protection plans to prevent data loss and restore business operations quickly. Thus, the network Managers' two most crucial jobs include developing an effective disaster recovery plan and managing the backup systems of the company.

Most often, the disaster recovery plans are not long, although the length also depends on the complexity of the network's operations. Consider a single network with several hundred nodes and perhaps fifteen servers; the disaster recovery plan prepared for this network will only be around ten to twenty pages long. If a network is a complex like the Fortune 500 companies, the plan for disaster recovery of all the sites considered in aggregate may be several hundred pages long.

The usefulness of the disaster recovery plan can be maximized by making it concise and relevant while keeping some focus on even the remote problems that have at least a small chance of occurring. Pay attention to the results of the disaster, such as loss of a single server or an entire server room, or loss of all the customer service workstations, etc., instead of worrying about the causes that lead to this disaster.

The minimum issues that should be focused on in a disaster recovery plan are elaborated in the following section. Depending on the company and the network being used, other related issues might also need to be addressed.

Assessing Disaster Recovery Needs

The disaster recovery plan should be drafted according to the needs of the company, i.e., the issues the plan should focus on and the person that requires the input into the process of recovery planning. Some other needs to be considered are:

- Considering various contingencies and formally planning for all kinds of possible disasters by designing countermeasures for them.
- Convincing the external accounting auditors of the company that a plan has been developed to counter the possible disasters.
- Making sure that the company's top management is notified about the risks and potential disasters, and the time it would take to deal with any problem that occurs.
- Developing a plan by starting from the key areas of the company's business considerations, including the different disasters related to the computer network.
- Persuading, the firm's customers that the data and operations of the firm are secure and safe from disasters.

Keeping these needs in view while planning will clearly show you what the plan should entail and which people from the different parts of the company should be involved in the planning process.

Considering Disaster Scenarios

To effectively prepare for disaster scenarios, and develop a plan, consider many probable disaster scenarios such as:

- A fire breaks out in a room, such as the server room, and destroys some computers and tapes.
- The computer and backup batteries close to the floor of the server room are damaged by flooding. It can occur by an incident within the building such as fire sprinklers activating due to a fire, or a serious case of water leaking into a room near the server room.
- A problem in the electrical circuits occurs, causing the power to fail.

- Connection to the outside world is lost due to some problem like the critical Wide Area Network (WAN) or the Internet connection going down.
- The network or servers of the company face problems due to bad building structure.
- The computers in another part of the building, essential for running the company's operation, get affected by the preceding events. It could be one of the manufacturing areas, the customer service center, or the telephone system room.

The events mentioned above do not have a high chance of occurring. However, it is still imperative to consider them all because a disaster recovery plan is made to deal with serious problems. If the planning is focused only on the problems most likely to occur, it will be much less useful.

Some failures which could endanger the system should also be considered after planning for disasters:

- The server's motherboard fails and a new one cannot be obtained from the vendor in less three days.
- The failure of a disk causes the loss of data. If using the scheme of Redundant Array of Independent Disks (RAID), make a plan that accounts for failures worse than the RAID system can protect. Such as, if RAID 1 mirrored drives are used, create a plan that considers the failure of both sides of the mirror simultaneously. For RAID 5, consider planning countermeasures for when two drives fail simultaneously.
- Consider a case where the tape backup drive fails, and repairs cannot be done within one or two weeks. This failure does not cause the loss of data, but it does increase the chances of such an event.

Planning for these failures requires ways of responding quickly and effectively. For example, if the server's motherboard fails, relocate the drives of that server to another one temporarily, until the motherboard gets fixed or replaced. If a disk fails, design a plan which contains a method to rebuild the disk array and quickly restore the data from a backup. If the tape backup drive fails, plan on how to obtain an equivalent drive soon, or if the tape-drive

developer can make an exchange of the failed drive for a reconditioned replacement drive.

Consider keeping spare parts and backup servers so that in case of any failure, system operation can be resumed quickly. Examine what these responses entail:

- Should a maintenance contract be kept close? If so, ensure that the guarantees and procedures are understood.
- Should spare parts be stocked and ready to use if a failure occurs?
- Is another computer available that can act as a temporary replacement for a key server if it fails? Can the same be asked for routers, hubs, switches, and other important components?
- Are the employees trained and ready to work with the replacements, or with no system if temporary measures have to be taken? For example, can a restaurant and its staff keep operating if the electronic system goes down?
- Is it necessary to maintain a hot or cold recovery site? A “cold” recovery site is a facility kept close to the protected data center and managed by the company. If the data center faces some disaster, the site can be hosted in this facility where all the power, air conditioning, and facility features are available. But the “hot” site has the same features as the “cold” site with the additional advantage of having computer equipment and software to perform the same processing as done in the data center. The data of the hot site is synchronized with that of the data center on a real-time basis, due to which it can take over the work of the main site in a short amount of time. Hot or cold sites are often used by those companies which need to carry out sensitive and mission-critical data operations.

The core of disaster recovery planning is based on two points; first, analyzing problems or potential risks, e.g., malfunctioning or failure of essential equipment, and second, after analyzing the risk managing it and overcoming the risk.

1. Handling Communications

The disaster recovery plan should cover the aspect of handling communication. If during a disaster, communication is not effectively planned, the people might not perform well at their jobs, and solving the crisis will be hampered.

Communication planning can be started by writing down the list of people that should be informed about a problem, how to track the progress made toward resolving it, and the result. An example list is given here:

- Board of directors
- President or chief executive officer
- Vice presidents of respective areas
- Supervisors
- Employees dealing with the problem

The next step includes deciding the notification that should be given to each person regarding the disaster recovery process. For instance, the board of directors may only need to be informed when the disaster progresses so much that it has a material effect on the performance of the company. But the supervisor and the employees directly affected by the problem need to be constantly notified about every development.

After considering the list of people and what they need to be notified about, decide the way they will be notified. If you are the one directly involved in solving the problem, consider passing on the responsibility of notifying the required people to another person not too directly involved so you can finish the process of resolution soon. This task should be delegated to your department's supervisor or an employee clear on the procedures required in communication. They should also have contact information such as home numbers, pager numbers, etc. if they must inform the person after working hours. Setting up a telephone tree will help to communicate with others quickly. The last task is to outline the order in which people are given the notification. This list depends on the company environment and the disaster, disregarding the organization chart of the company.

1. Planning Off-Site Storage

Off-site storage is a method of protecting data by keeping it in

back-up tapes in an off-site place if a physical disaster like a fire destroys the copies of data present on-site.

Along with off-site storage of files, companies also provide standardized tape-storage practices that work on a rotation basis (most often weekly). The employee of the storage company visits the office and exchanges boxes by dropping one box of tapes and picking up the next set of tapes. The backup tapes are commonly contained in stainless steel boxes, and the duty of keeping these boxes locked and guarded is given to the network administrator. The decision as to which tapes to keep on-site and which to send off-site should be made carefully, like keeping the most recent backup tapes on-site and sending the older ones off-site. This is helpful, as you can keep the tapes you need daily close to you while reducing the exposure to disaster. Even if a disaster damages the server room and backup tapes, only the recent data will be destroyed, which does not amount to much loss.

1. Describing Critical Components

The plan developed for disaster recovery should also include all the computer equipment and software needed to keep the operations running should the entire building be lost. The roughly estimated cost of this equipment and the method of obtaining it quickly must all be a part of this plan. Such a list will help reduce the time lost in resuming the business operations in a temporary facility. The insurance purchases made against business operations will also be estimated in the total end cost.

1. The Backup and Restore Features of Networks

An inclusion that the disaster recovery plan for a network must have is the method of recovering the stored server data if it gets destroyed. One such method is establishing network backup and restore procedures. A network administrator should know the importance of keeping reliable backups of important data and the system itself.

When a person works with computers, it doesn't take long for them to notice the importance of keeping good backups, because computers can fail unexpectedly, making recovery of the data inside them impossible. Some files on the computer may also get deleted or corrupted due to an incident. If such cases occur, the company

employees' jobs depend on the quality of backups for the destroyed data and the restoration of that important data.

Assessing Backup Needs

Assessing the needs of a company's backup and restoration process comes before making the backup procedures for a network. To complete the assessment of backup needs, consider these questions:

- How dynamic is the server data, and with what frequency and in what ways does this change?
- What is data that needs to be backed up, and what is the growth rate?
- How much time does it take to make the backup of the data? Avoid a situation where you back up terabytes of data on a system that can only handle megabytes per hour.
- How quickly can a partial or complete restoration of data be done? Most often, the restoration of data takes twice if backing up the same data, though there are cases where the backup and restoration time is equal. For example, if the entire server took ten hours for backup, then the restoration data would be somewhere between ten to twenty hours, excluding the time needed to deal with the problem that led to having to restore the data.
- How much consistency in the backup data is required? Are the data files required to be managed as one unit? For example, the restoration of word processing files need not be coherent and will not impact other files in the system. However, a collection of database files from a high-end database is useful only if the files can be restored from the set from the same point.
- What compromise can be made between cost and recoverability? A backup system designed to backup files every minute can create high confidence in the fact there is no loss of data even if some issue arises. Such high-end backup systems are required in banks. But the cost and administration of such backup systems are high, and most companies might turn to some cheap alternative with a low degree of recoverability

such as backup at off-hours (usually at night). A company can assess what it needs and how much it will spend.

- How many extra levels of backup are required by the company? The backups are mostly in tapes that support servers that use RAID arrays. In this way, the second level of protection is the tapes. Sometimes, multiple copies of the tapes are required, and each copy of the tape has a backup. Maximum redundancy can proceed by copying backups and keeping them at an off-site via some network connection.

When the assessment is to be made, the company's senior management must be involved. On a minimum level, the findings can be presented for seeking the agreement or input of the management.

Acquiring Backup Media and Technologies

These factors should be considered when a backup system (hardware and media) is being chosen.

- Reliability
- Cost
- Capacity of storage
- Probable restoration frequency
- Fitting an entire backup into a single media

The following information relates to various backup technologies, their costs, and the pros and cons of each one. All the values such as prices of drives, media, and costs per megabytes, are based on approximations.

Digital Linear Tape (DLT) or Linear Tape-Open (LTO) are sturdy backup systems that should be considered if your company has adequate resources and ways of using their capacities. These systems are rated for re-use a million times, with a shelf life of 30 years. and have fast drives for backup and restoration. DLT and LTO can also have robotic autochangers, which make a lot of headroom if the drives are being filled up. These robotic autochangers are comparatively cheap, and various types are available, ranging from small systems with a capacity of five tapes to large systems holding

tens to hundreds of tapes.

Super DLT S4 with 600GB per tape and LTO-4 with 800GB per tape are new backup technologies more advanced than DLT and are suitable for larger networks. A lot of computer equipment vendors support the tape formats of DLT and LTO and consider them to be reliable.

Choosing Backup Strategies

The backup rotation strategy is planned after all the important information is collected, and this plan contains the details of how the backup media is rotated. Thoughtful designing of these backup rotations has these advantages:

- If a disastrous failure occurs, the system can be rebuilt based on the most recent data possible.
- If old tapes have been accidentally erased or damaged without being noticed they can have their files restored immediately before the data is lost.
- Provide protection if the backup media fails.
- Protect the data against cases of environmental disasters like a fire.

The files on most network operating systems have special bits assigned to them, one of which is called the archive bit, and it specifies the backup status of the file. The archive bit is set to 'on' whenever a file is edited, indicating the need for a backup of this file. Once the backup is done, the archive bit clears. With archive bit and backup software, the backups that can be created are:

- A **full backup** in which all the files and directories are backed up with no regard to the statuses of the archive bits. This method clears up all the archive bit on every file in the backup.
- An **incremental backup** selects those files modified and had their archive bit on, and then creates backups for these files. The only files backed up are those that have been edited since the last incremental or full backup, and their archive bit is reset; those who have not been modified will not be included. Though the time consumed in incremental backups is minimized in

each daily backup, the restoration time is increased, and the possibility of media failure becomes high.

- A **differential backup** works by backing up those files which have their archive bits set to on. The change in this backup is that the archive bits of the files are left on even after a backup so that in subsequent backups, they will be backed up repeatedly along with other new modified files. The time taken in performing backups is increased, but the restoration time, and the possibility of media failure, is reduced.

Ideally, performing full backups is advantageous as you have to access only the most recent backup tapes to restore the system if a failure occurs. Looking at it realistically, such a thing is not feasible due to several reasons. First, to perform a full backup is time-consuming, and there may not be enough time to do a full back up daily. Second, the less work is done by the tapes and media, the more shelf life they will have. Besides these concerns, consider much restoration time the combination of a full and incremental or differential backup will take along with the risk of being unable to restore the data due to using a combination approach. Also, consider the scenario where you need a full restoration, and you have to use one full backup tape and four incremental backups used since then. All the five tapes need to be in good condition, which is less likely than encountering a bad tape.

It is common to mix the backup types by performing one full back up in a week and using the incremental or differential backups for the rest of the week. Some examples are:

- **Full back up Friday nights and incremental backups from Monday to Thursday:** Due to system failure on a Monday morning before any data entry, only the Friday's full backup needs to be restored. But if the failure happens on Thursday, four tapes need to be restored in sequence for a complete backup, starting from Friday's full backup and continuing from Monday's incremental backups till Wednesday. In the second case, all the data in those tapes must be restored successfully and sequentially to ensure data integrity. If it is not done, the files might become mismatched and hard to use. Hence four points of

media failure in the form of tapes increase the risks more than you can handle.

- **Full back up Friday night and differential backups from Monday to Thursday:** if system failure on Monday morning occurs, only previous Friday night's full backup restoration is needed. But if it fails on a Thursday Morning, complete restoration of data required only two tapes: the previous Friday's full back up with the differential backup done on Wednesday. This is because, in the differential backup, all the modified files since the last backup have been backed up, and so, the number of possible media failure points decreases due to only two tapes needing to be restored.

A good backup scheme needs a balance between the data's nature and the risks with each backup, the tapes' capacity, and the time consumed in each backup.

The 'Grandfather-father-son' (GFS) scheme is the most common backup rotation scheme. Eight tapes are used in implementing this scheme. Four of these tapes are named from "Monday" to "Thursday," while the other four are "Friday 1", "Friday 2", "Friday 3," and "Friday 4". The first four are used from Monday to Thursday to replace the data from the previous week, while the next four tapes are designated for each Friday in the month. For the first Friday in the month, use the "Friday 1" tape and so on. Prepare a month-end tape on the last day of each month, not for being re-used but for keeping it off-site so it can be used where a crisis like an environmental failure destroys the system and all the on-site tapes.

GFS has three main variations:

1. Perform a full back up each time, which increases media redundancy but reduces restoration time.
2. Perform full backups only on Fridays and the end of the month, and during the rest of the weeks use incremental backups.
3. Perform full backups on Fridays and month ends, and during the weeks perform differential backups.

Compared to GFS, rotation schemes are simpler; only two or three tapes can be used by rotating them in a sequence and

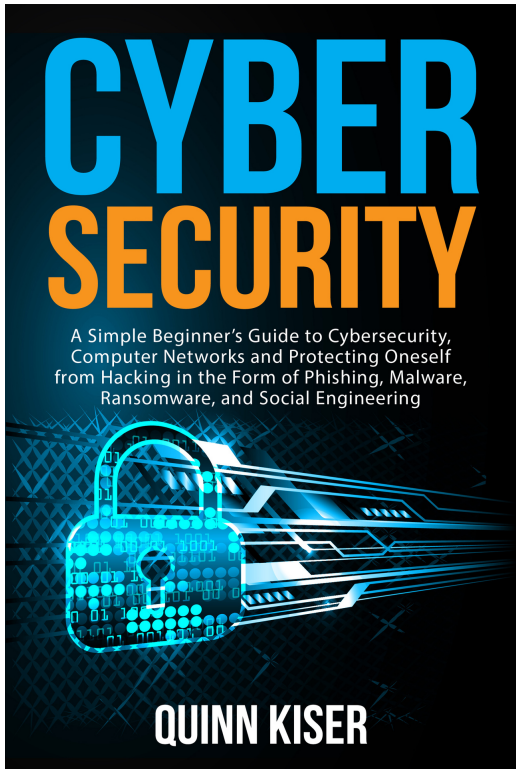
overwriting the old data each time. In this way, the three previous days' data can easily be restored. But it is impossible to retrieve data from further back in time if it was erased or damaged with no one noticing immediately. A way of solving this shortcoming is by using several more tapes that can be rotated weekly or monthly.

Conclusion

Until now, we have covered a variety of topics related to computers. We have comprehensively discussed computer networking because it is very relevant in our modern age ruled by the Internet. We have learned about the OSI networking model and how the different protocols and networking applications adhere to this model. After addressing computer networking, we shifted our focus toward network security, which is a very important topic to discuss as nobody wants their data to be compromised and misused. In the final portion of this book, we have given due importance to topics such as network designing and hacking, with the latter being more interesting and informative. Hacking is something anybody with the right tools and knowledge can do. This book has explained the general process of hacking, which is commonly called the 'kill chain process.' the book has given readers the best of each topic and hopes that the readers have developed a basic conceptual foundation of each topic discussed in this book. When studying any material that relates to the topics covered in this book, the reader will have enough background knowledge to readily digest information meant for an intermediate or advanced-level audience.

Part 2: Cybersecurity

A Simple Beginner's Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering


CYBER
SECURITY
A Simple Beginner's Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering
QUINN KISER

Introduction

The Internet may be the most important invention of the twenty-first century, and it affects people's lives daily in more ways than they realize. Everything has changed since the invention of the Internet—the way you communicate, play games, shop, work, listen to music, watch movies, pay bills, order food, and even the way you make friends. Think of anything you want, and there is probably a mobile or web-based app for it.

The Internet has made people's lives very comfortable. You do not need to stand in a queue or write a check to pay a bill anymore. You can just get done it at the click of some buttons. Technology has advanced to such an extent that millions of devices are capable of connecting to the Internet—most don't need to be connected to your computer. There are smartphones, tablets, etc., through which you can stay connected to your friends and even work whenever you want.

The Internet has not only simplified things but also made them cost-effective due to how it is used not only by the rich but all classes in society. In the past, people had to think very hard before making international calls because of the charges imposed by telecom providers. Today, you can use the Internet to make standard and video calls at great rates, even free in some cases, anywhere in the world.

The Internet has also changed the adoption rate of traditional devices like television, as people now prefer to watch everything through a subscription model on the Internet. People do not use a mobile phone just to make calls anymore, but tons of other activities, such as watching a movie, booking tickets online, etc. The Internet has even made it possible to work from home, which is convenient for parents as they can keep a watch over toddlers at the same time. In other words, people have become closer since the arrival of the Internet.

However, the Internet has made way for new kinds of crime, too, known as cybercrimes. While the Internet became the "in place" for people to hang out and socialize, it also offered cybercriminals massive opportunities. Criminals realized that with everything going digital, they also needed to adapt and go digital too. It did

not take them much time to understand that the entire world uses the utilities provided by the Internet for activities such as shopping, banking, ordering food, etc., and that all of these have a common twist—financial transactions over digital media. Billions of dollars, British pounds, and thousands of other currencies are moved around via the Internet these days, every day, and that is a huge attraction to criminals, providing an alternative way for them to commit their crimes.

A thief does not need to walk into a bank anymore to steal money; it can be done over the Internet. This led to the arrival of cybercriminals who commit crimes over the Internet known as cybercrimes. In this book, you will learn about all kinds of cybercrimes and how cybercriminals implement them.

If there is a law in the real world to keep a watch over criminal activity, there are processes in the digital world to keep cybercrimes under control. Cybersecurity is a hot term used on the Internet, and that is what this book is all about. You will learn about the various ways through which you can use cybersecurity to counter cybercrimes.

By the end of the book, you will also have read about security testing and the careers you can have for yourself in the cybersecurity domain if you are an aspiring student or looking to switch your field from your current profession. This book will open your eyes to new possibilities and bring out the digital version of Sherlock Holmes residing within you.

Chapter One: Cybersecurity and Why It's Important

What is Cybersecurity?

Cybersecurity, also known as information security, is defined as the process of ensuring ICA of information, where I stands for Integrity, C stands for Confidentiality, and A stands for Availability. Cybersecurity comprises a set of relevant tools, approaches toward risk management, training, technologies, and methods to protect the information, networks, programs, and devices against attacks and unauthorized access.

The following entities are part of the cybersecurity process.

People

People are part of a system. It could be a university or an organization or another institution. During their tenure with an institution, people should understand and comply with the basic principles of data security, such as using strong passwords, being alert about email attachments, and doing data backups.

Processes

Organizations need to have certain frameworks in place to tackle cyberattacks, both attempted and successful ones. If an organization has even one well-respected framework, it can guide them in times of a cyberattack. A framework will help them identify the attacker, protect all systems, be response-ready for threats, and quickly recover in case of successful attacks.

Technology

Without technology, organizations would not have the necessary tools for computer security to protect themselves against cyberattacks. There are three main entities to protect: personal end-point devices—such as smart devices, computers, and routers—the network, and the cloud. The common technologies used to protect these entities include firewalls, DNS filters, anti-malware solutions, antivirus solutions, and email security solutions.

Why is Cybersecurity Important?

Today, the world depends on technology more than it ever did in past decades. This has resulted in a huge surge in the creation of digital data. Data is stored on computers by individuals, businesses, government agencies, etc., and daily transferred to other computers over a network. There are loopholes and vulnerabilities in computers and their underlying systems. These can be exploited by an attacker, which leads to the downfall of an organization. This is why cybersecurity is vital.

A breach in the system that allows an attacker access can have far-reaching consequences. The leak of customer data can affect the organization's reputation and lead to a loss of trust with partners and customers. Theft of software source code can cost the organization a competitive advantage over its rivals. Additionally, a data breach can cause revenue losses due to data protection practices being non-compliant.

On average, a data breach can cost an organization up to USD 3.6 million. Moreover, high-profile data breaches make it into the news headlines like wildfire resulting in a hit on a company's reputation. This is why organizations need to implement a strong and powerful approach to cybersecurity.

Cybersecurity Scenarios

This section discusses the need for information security. You will go through a few common scenarios in which cybersecurity is used in the world today.

Scenario for Organizations

Try to picture an organization with all the latest IT equipment to cater to all their digital needs for their business to function smoothly. It is critical for this IT infrastructure to be up and running around the clock. The organization also needs to ensure that the identity of the data, network, equipment, and products are secured, except for public-access network and data identities. However, the public data itself must still be encrypted and secured. All organizations have gone digital, and therefore there is a mix of various technologies working together to drive the goals and objectives of an organization. Digitization also extends the boundaries of an organization, thereby increasing their connectivity. The connectivity is, of course, an advantage today but can be harmful to the organization.

Three macro aspects define digitization and connectivity:

● Identity – This is an aspect through which users can interact.

● Data – This is data related to the user, business, system, or customer.

● Network – This is the part where everyone is connected and restricted via access levels.

These three macro entities are connected via equipment, software, and business processes. As already mentioned, an organization controls the level of access a user may have to create, view, or modify data via access developed for an identity. Additionally, data—whether it is in rest or motion—also needs to be secured. And finally, it goes without saying that the network perimeter for this infrastructure, whether it is in a physical form or on the cloud, requires security.

The Scenario Where Everything is Moving to the Cloud

What is the cloud? A cloud is a common space on the Internet where all your data can be stored instead of storing it locally. Most organizations are rapidly moving all their data to the cloud. This happens because cloud-based servers offer better computing power, and the cost of storing data on the cloud is less than storing it locally. Another benefit of cloud-based infrastructure is that it is scalable. This means that its parameters such as RAM, computing power, and disk space can be expanded on the go.

With the Internet, the world is getting smaller, and organizations have started collaborating on a global scale, and cloud computing is to be credited for this. Gone are the days when employees would sit in an office and work. Today, employees prefer working out of remote locations, thereby eliminating the need for a physical office. Cloud infrastructure also takes away the burden on local IT teams to constantly keep a watch for software and hardware upgrades.

Cloud infrastructure has definitely brought in a new era of more speed, control, accuracy, power, and availability, but many security risks also accompany it. Cloud infrastructure is no different vis-à-vis security, and disasters can happen if that infrastructure is not secured properly. The biggest advantage of cloud infrastructure is that an organization does not have to own or maintain infrastructure. However, the boon is accompanied by concerns such as how do you secure it? Who has access to the data present in the cloud? How do you keep the cloud compliant with government regulations such as PCI or GDPR?

The service provider's business model also governs the disaster recovery policy around cloud infrastructure, and therefore an organization needs to be up to date on this. The organization does not have any say in where the service provider's data center is located. There are several other risks and challenges to using cloud infrastructure, which will be discussed in the next few chapters.

Cybersecurity Terminology

Several terms used throughout this book relate to the cybersecurity domain. It is important to cover these terms in the first chapter so that you are familiar with them when they start making subsequent appearances. These terms are related to all the devices you use today, the software on those devices, the network infrastructure the devices are connected to, and so on. You will now go through these terms individually.

Cloud

The Internet is made up of clouds—and not the ones in the sky. Cloud computing is a technology that allows a user to access their files from anywhere in the world. Cloud is a network of computers that store data that can be accessed by a smart device remotely. The most common example of a cloud is your emails. They are stored on a distributed set of computers on the Internet, and you get to access them from anywhere as long as you have the required credentials. Another example would be something like a Spotify playlist that you have created using your mobile phone, but you still get to access the same playlist from another device like a laptop when you log in using the same account.

Software

The software can be defined as instructions that tell a computer what to do. These instructions are put into a package known as software, which a user can install and start using. One of the most common software examples is Microsoft Office, which is used to create documents, presentations, etc. Your smartphone apps are also software that you use for various purposes. For example, WhatsApp messenger is the most common app used to send messages.

Domain

A domain is a parent for child devices that are interconnected, such as computers, smartphones, printers, etc. For example, all the computers at a workplace are a part of a domain belonging to the organization. There are policies defined in the domain's framework

that govern the type of access that the devices will have under that domain.

IP Address

An IP address is a digital address assigned to a smart device over a network, which can be a local network or the Internet. Every device connected to a network is associated with an IP address. That IP address is used by other devices to locate and communicate with each other.

Virtual Private Network (VPN)

A virtual private network is a network over which you can be anonymous. You get assigned an IP belonging to a different region, and all your actions over the Internet are logged via that IP, thus keeping your original IP hidden. VPN applications also encrypt the traffic for you so that the Internet Service Provider or the government cannot track your activities online. VPNs are also used by organizations to keep you connected to the office network if you want to access the office network from outside. This has gained a lot of popularity in recent times as it helps a person work from home or remotely.

Exploit

An exploit is defined as a malicious piece of code that can be used to take advantage of a vulnerability or loophole in a computer or a server. Viruses, Trojans, Botnets, etc., are all used to execute an exploit in a target system.

Breach

The moment when an attacker takes advantage of a system's vulnerability, and gains access, is known as a breach.

Firewall

The technology used to create rules for a system, so incoming and outgoing traffic can be filtered, is known as a firewall. Firewalls can be implemented using both hardware and software.

Malware

Malware is a broad term or an umbrella that includes any malicious software that can harm a computer. The most common types of malware are viruses, worms, Trojans, ransomware, etc.

Virus

A virus is defined as malware that can harm certain programs on a computer. It can further replicate itself and spread over multiple files and computer networks. It needs a host file and cannot execute

by itself. Viruses were known to affect only software, but they have evolved in recent years even to cause physical damage to hardware.

Ransomware

Ransomware is a type of malware that will encrypt all the data on your computer and prevent you from accessing it. The attacker who deployed the ransomware will leave an application where you make a payment to them, after which the files will automatically be decrypted. In 2017, a ransomware known as WannaCry infected all Windows-based machines.

Trojan Horse

A Trojan horse is like a virus, but it does not execute by itself. It is usually masked and lies under a file, which may be important to a user. For example, a user may receive a PDF with the content they were expecting, but at the same time, clicking on that PDF triggers a malicious script. This implementation is known as a Trojan horse.

Worm

A worm is a piece of malicious code that is capable of replicating itself over a network. It may not necessarily infect a file like a virus does, but it can do something annoying like consuming the network bandwidth and denying the bandwidth to the user.

Bot or Botnet

A Bot is a malicious application that can be planted over a network of computers, allowing an attacker to remotely take control of the complete network. The collection of computers on which the bots are planted is called a botnet. The botnet is controlled by an attacker who is known as bot herder.

DDoS

DDoS stands for Distributed Denial of Service and is a form of cyberattack. The motive of a DDoS attack is to flood a network with malicious traffic so that genuine requests for a website cannot be accommodated in the bandwidth. DDoS attacks are often executed by implementing botnets.

Phishing and Spear Phishing

This is a technique that is used by attackers to retrieve information. The most common example of this is emails sent to unsuspecting users, which may seem legit but will have links redirecting you to something else. For example, if you have an account with Citibank, the sender of the email will have an email

address like something@citibanks.com, adding an extra S. An innocent user may believe it to be legit and may end up clicking on a link they are not supposed to. These links can often ask you to enter your account details and even login passwords that will be recorded by the attacker.

Encryption

The process of encoding data using a known algorithm so that no one can access it, except someone with a decoding key, is called encryption.

Bring Your Own Device (BYOD)

This is a policy implemented by many organizations that suggests that employees can use their personal devices for business. A BYOD policy will have access restrictions concerning whether the personal device can connect to the corporate network or not.

Penetration Testing

Penetration testing—also known as a pen-test—is the process of using attacking tools and techniques to review the security of an organization's infrastructure. Internal teams or external experts are hired to conduct the test to discover vulnerabilities in the organization's infrastructure so that they can be fixed before encountering a real attack.

Clickjacking

This is an attack that tricks the user into clicking on a link or button, which looks genuine but has malicious scripts embedded in it.

This book has only covered the tip of the iceberg for cybersecurity terminology, but this will serve as a launchpad to better understanding.

History of Cyberattacks

In this section, you will go through the most well-known cyberattacks in history. Cyberspace is an open community where everyone is connected and can reach anyone irrespective of time or distance. It may be called a way of life today, but if not used with care, it has consequences. There are notorious people in the world who use cyberspace to attack websites belonging to banks, social media that contains a gold mine of user information, and even

governments. Here are a few modern cyberattacks.

The SpamHaus Project

SpamHaus is a public service on the Internet that helps filter out spam emails based on their content or the reputation of their origin. The attack on SpamHaus is considered to be the biggest cyberattack in history where home and business broadband router owners were targeted. The attackers gained control over these routers, and all these users became involuntary participants of the attack. Millions of email service providers use SpamHaus to filter out spam emails from the Internet. On March 18, 2013, SpamHaus had blacklisted a company called Cyberbunker, which led to losses for the company. Cyberbunker and other hosting companies retaliated to this by hiring hackers who deployed botnets by exploiting broadband routers to shut down the SpamHaus network.

Sony Playstation

In 2011, information such as credit card details and user information was stolen from 77 million users by a group of hackers. This cost Sony around USD two billion in damages. Another pain point for the company happened when hackers were continuously able to access the Sony network using the login details of gamers even when the company was trying to fix the issue. This whole attack lasted for twenty-four days.

PayPal

In December 2010, PayPal became a victim of a cyberattack. This happened immediately after PayPal had blocked the account of WikiLeaks for fundraising, citing violation of PayPal's acceptable usage policy. Multiple users boycotted PayPal because of this event, and many hackers started targeting PayPal.

Canadian Government Hacking

In February 2011, the Canadian government disclosed via multiple news channels that they had become victim to hacking conducted from IPs that were traced back to China. The attackers were able to access three departments of the Canadian government and stole data from those departments. The attack was eventually stopped by cutting off Internet access to these three departments, putting a full stop to the transmission of data to China.

4chan

4chan is an English language based website used for posting pictures and discussing Japanese anime and manga. It was launched

in October 2003 by a fifteen-year-old New York student named Christopher Poole. The users were allowed to post anonymously, which served as a drawback for the website. A user, Hal Turner, claimed he was the target of DDoS attacks and prank phone calls made to his radio show in 2006. In 2008, an anonymous 4chan user hacked the private Yahoo mail account of Sarah Palin, a candidate for vice-presidential elections.

Citigroup

Citigroup is one of the largest financial institutions in the world. On its own, this was enough incentive for notorious attackers to target their network as it had a lot of sensitive and valuable information flowing through it daily. An attack in 2011 on the Citigroup network led to customer information, such as contact details and account information, being stolen from more than 200,000 customers. The company suffered monetary damage of USD 2.7 million due to this attack.

Michael Calce

In 2000, a fifteen-year-old boy named Michael Calce, popularly known as “Mafiaboy” in cyberspace, gained the spotlight for hacking high-profile companies such as computer giant Dell, Fifa.com, Yahoo, Amazon, CNN, and eBay, causing damage worth USD 1.2 billion. He also attacked nine out of thirteen root name servers of the Internet domain space. Being a juvenile, Calce got away with only eight months of open custody, a year of probation, and a small fine. He was also not allowed to own any Internet-powered device by the Montreal Youth Court for eight months.

Chapter Two: Cyberattacks and 10 Types of Cyber Hackers

The Internet that you know today came into existence in the 1960s, and it was only accessible to a few scientists, researchers, and the Defense Departments at that time. However, the user base for the Internet has evolved exponentially ever since. In the initial days, a cybercrime was described as physical damage to a computer and its infrastructure. This definition of cybercrime changed in the 1980s to include using a virus that would cause a computer to malfunction.

The effect of cybercrime was marginal back then as the Internet was limited to mostly defense setups, large organizations, and research communities. The Internet was launched for public use in 1996 and was instantly popular with the masses to the point that it changed their lives. The Graphical User Interface for the Internet was designed simplistically, making it easier for users to understand the functionalities and characteristics of the Internet. Life was simple, and users only had to click on hyperlinks or type URLs into the browser without having to think about where the data on their browsers came from. They did not need to worry if anyone else had access to the data or if the data they received was snooped or tampered with by an attacker. As the Internet evolved, cybercrime's focus shifted from merely damaging a computer physically or interfering with data to committing financial crimes.

The Internet was at its peak by 2013, and the rate at which cybercrimes were being committed increased rapidly. Twenty-five computers became victims every second, and an estimated 900 million users were already victims of cybercrimes. With almost everyone in the world now owning a smartphone, the number of victims has vastly increased.

Classification of Cybercrimes

Most cybercriminals attack organizations since most organizations maintain a database or server with large volumes of sensitive data about their employees and customers. A cybercriminal can either be an outsider or an employee of the organization. You can classify cybercrimes into two kinds based on this criterion.

Insider Attack

An attack on a system or computer infrastructure by someone who already has access to it is an insider attack. The attacker, in this case, is either an employee or a consultant working in the organization. These attackers perform the hack for various reasons, such as greed and revenge. An insider can perform an attack on the system easily since he or she is aware of the infrastructure, policies, and the weaknesses of the security system. This individual also has access to the organization's network. Therefore, it is relatively easy for an insider to steal information or harm the infrastructure. An insider usually finds a window of opportunity for an attack, especially when they are assigned new roles in the organization. For example, when a company develops a new application, it may not have the necessary controls and policies in place to secure the data in the application. An insider can use this vulnerability to perform the hack. Insider attacks can be detected and prevented by installing intrusion detection systems internally within the organization.

External Attack

External attacks arise when somebody inside or external to the organization hires a hacker to attack the organization's network and systems. External attacks are executed to cause financial and reputational losses to an organization. An external attack needs more planning and research when compared to an insider attack. Every external attack goes through the following stages:

- Planning
- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access

If the organization's network admin is experienced, he or she constantly checks the firewall logs and scans the systems and network to identify vulnerabilities. The organization can also use intrusion detection systems to detect and prevent external attacks.

In addition to insider attacks and external attacks, there are two more types of cyberattacks: structured or unstructured. This classification is based on the experience of the attacker. Most people classify these attacks as external attacks, but there are cases

where an employee has performed structured attacks on the organization for personal gain. These types of attacks are often carried out by rival companies. They may send one of their employees to the company and ask them to collect information from that company. This is known as corporate espionage.

Unstructured Attacks

An attack carried out by an amateur attacker without any predefined motive is classified as an unstructured attack. These attacks are often carried out using a penetration tool readily available on the Internet. The attacker may use this tool on the company's network.

Structured Attacks

A structured attack is planned and executed carefully by an experienced and skilled professional with clear objectives. Attackers have access to powerful tools and technologies that help them access the target system or network without being detected by an intrusion detection system. Additionally, an attacker also has the knowledge required to modify an existing tool to suit the specific attack requirements.

Reasons for Cybercrimes

An attacker can choose to hack a system or network of an organization for multiple reasons. The following are some common reasons why cybercrimes happen.

Money

Attackers commit cybercrimes to earn money since this is an easier and faster way to make money. They use hacking methods, such as phishing and spoofing, to trick someone into revealing their account information. The attacker can use this information to transfer the funds from the victim's account into their own.

Revenge

Some attackers may want to take revenge against another individual, organization, religion, or government. They may choose to hack these entities to cause financial and physical losses. This form of attack is known as cyberterrorism. Some attackers hack systems and networks when they want to test a new tool or software. The only objective of such an attack is to understand how the new tool or software works.

Recognition

Some attackers choose to attack to gain popularity. They may hack a defense or large organization's systems and networks to make a name for themselves—anonymity.

Cybercriminals can ensure their anonymity when they perform a hack. It is extremely easy for cybercriminals to get away with their attack since nobody knows how to trace the attack back to the cybercriminal. This anonymity, at times, has even motivated respectable citizens to commit a cybercrime for personal gain.

Cyber Espionage

Some governments may choose to overlook the data privacy act and track everything their citizens do. They may choose to do this for political or economic reasons.

Types of Cyber Hackers

Hackers are curious about how networks and computer systems work. They are skilled in coding and programming since they do their best to hone their programming skills. They also learn about various tools and technologies they can use to perform hacks. Since hackers attack an operating system, they learn more about the different kinds of systems and find their way around the system to identify any vulnerability.

Here are the most common types of hackers.

White Hat Hackers

Hackers who have certifications and are authorized to conduct penetration tests for an organization or a government to identify vulnerabilities in their information systems are white hat hackers—or also known as ethical hackers or cybersecurity experts. They are a part of the security team in an organization, and their job is to prevent an attack on the organization's system and network. They comply with the rules of engagement stated by the organization or government.

Black Hat Hackers

Black hat hackers, also known as crackers, want to access your system and network and steal, manipulate, or destroy your data. They implement common hacking practices for their attacks. They are lawbreakers or criminals, and it is easy to differentiate between a white hat and black hat hacker based on their objectives.

Gray Hat Hackers

These are hackers that fall in a spectrum between white hat and

black hat hackers. Since they are not certified as cybersecurity experts, they can choose to work for or against the organization. The motives of the hacker determine whether he is a white hat or black hat hacker.

Script Kiddies

Script kiddies are known to be the most dangerous people in the hacking world since they lack experience and knowledge. They use any malicious tool or software available on the Internet without learning what it is used for. They also have no idea about the damage they can cause to the network or system. They attack computers and networks intending to mark their presence in the hacking world.

Green Hat Hackers

Green hat hackers are also amateurs of the hacking world, but there is a difference between them and script kiddies. They have little knowledge about hacking and work on developing the necessary skills to hack since they are passionate about becoming professional hackers. They are inspired by other professional hackers and keep in touch with them to learn to hack.

Blue Hat Hackers

Blue hat hackers are script kiddies who have some knowledge about hacking. They are different from green hat hackers since they perform a hack with malicious intentions. However, they do not have the intention to develop the necessary skills to carry out the hack.

Red Hat Hackers

Red hat hackers, also known as eagle eye hackers, are like white hat hackers. They do their best to counter any attacks carried out by black hat hackers. The difference is that red hat hackers are ruthless and destroy the network and systems used by black hat hackers.

State-Sponsored Hackers

As the name suggests, a country or state hires these hackers to hack into other countries' or states' systems to extract defense-related information. They are on the government's payroll.

Hacktivist

The online version of an activist is known as a hacktivist. They are anonymous hackers, and they target government systems for social and political reasons.

Whistleblower

An employee of a government or organization who feels their institution is being unethical and conducting illegal activities may choose to call it out against their conscience. They may also do this for personal gain. Such hackers are known as whistleblowers.

Common Tools Used by Hackers

Hackers use numerous tools to execute the perfect attack. The following are the most common tools in a hacker's toolkit.

Rootkit

A rootkit is an application or a set of tools that allows hackers to gain remote control of a computer or network of computers connected to the Internet. The rootkit was originally developed to open backdoors in any software so that it could be fixed or updated with patches. Hackers tweaked this application to suit their needs. They now use this tool to control the operating system.

Rootkits can be installed in various ways on a target system. The most popular methods are phishing and social engineering. Once rootkits are installed on a target system, the hacker can control that system. They can destroy or steal sensitive information from that system.

Keyloggers

Keyloggers are tools capable of recording every key pressed on the keyboard. Keyloggers cling to the Application-programming Interface of any application and record every keystroke made by the user when they access the application. The recorded keystrokes are saved to a file that contains sensitive data, such as usernames, passwords, website URLs, opened applications, etc.

Keyloggers are scary as they can record credit card details, mobile numbers, personal messages typed in email applications, etc., provided they were typed using the keyboard. Keyloggers are planted using malware such as Trojan horses on a target's computer.

Vulnerability Scanners

As the name suggests, a vulnerability scanner is used to scan networks and computer systems to identify vulnerabilities or gaps. Ethical hackers commonly use this tool to identify loopholes in a system so they can patch them as soon as possible. Black hat hackers also take advantage of vulnerability scanners to discover

weaknesses in a target's system or network to exploit them.

Types of Cybercrime

It is also important to understand the crimes a person can commit using digital platforms, such as computers and the Internet. Here are the various types of cybercrimes people commit today.

Cyberstalking

When someone uses the Internet to stalk another person, harass, or threaten them, it is cyberstalking. A cyberstalker often uses applications like email, online messengers, social networking websites, etc., to execute cyberstalking. These mediums offer anonymity. Cyberstalking includes activities such as sexual harassment, monitoring someone's private life, false accusations, etc.

Forgery/Counterfeiting

It is a crime to counterfeit documents. With advanced applications available today, it is easy to create a document that looks exactly like the original. It becomes difficult to differentiate between the correct and fake documents unless you are an expert.

Child Pornography

Possessing, uploading, or downloading the sexual content of a minor is a cybercrime. Multiple websites on the Internet promote child pornography and exploit many minors in the world.

Cyber Terrorism

Some people use digital resources to spread hatred against a religion, country, etc. This is an act of terrorism and is known as cyber terrorism.

Piracy

Content is available digitally today and can be easily copied and distributed over the Internet. Distribution of content owned by someone else is illegal. For example, the illegal distribution of movies or music over the Internet is classified as piracy and is a cybercrime.

Computer Vandalism

Destruction of digital resources, either using physical means or malicious code, is computer vandalism and a cybercrime.

Phishing

Phishing is the process of tricking someone into disclosing their sensitive information, such as bank account details, via email. The attacker sends an email that resembles emails sent from a bank or other financial institutions using a domain similar to the bank's domain. The attacker can ask the victim to provide sensitive information, such as their account number, password, etc. The attacker can then use this information to transfer funds from the victim's account into theirs. If the hacker performs the attack using a telephone, it is known as vishing or voice phishing.

Hacking

Hacking is the act of accessing a computer that does not belong to you to steal, modify, or destroy data present on it. The motive behind performing a hack can be political or social.

Spreading Malware

Some hackers use different websites to spread malware. They may do it for fun or have certain objectives. Malware can destroy systems resulting in financial losses for a business or individual. The losses include the cost of repairing the system and the data destroyed. If the hacker is found, the business can sue them for damages.

Cross-Site Scripting

Some notorious attackers inject a client-side script into the website's code. An innocent user who visits this website ends up executing this script, and the script scans the cookies in the user's network. The script uses the cookies to collect sensitive information and transfer that information to the attacker's system. The attacker can use this information to gain access to the user's computer or sessions on a website and use it to exploit the user financially.

Spamming

The act of sending bulk unwanted and unnecessary emails over the Internet is spamming. An email can be called spam if it is one of the following:

- Anonymous: The sender remains anonymous.
- Bulk Mail: The sender sends one email to multiple users.
- Unsolicited email: The sender did not request the email.

Spam emails not only congest the victim's inbox, but they also congest the network.

Cyber Squatting

The act of registering a domain using a trademark of another organization with the intention of later selling it to the organization that owns it for a high cost is cybersquatting.

Online Auction Frauds

Various websites on the Internet conduct online auctions, and cybercriminals take advantage of these websites. They clone the website, and any payment made during the auction moves to the hacker's account.

Internet Time Thefts

Internet time thefts are mostly a crime of the past where an attacker steals a user's Internet Service Provider (ISP) details and uses that information to surf the Internet at the cost of their time. This means the user is charged for the time spent on the Internet.

Web Jacking

Web jacking is when an attacker hacks an organization's website to display irrelevant information. They may also use this opportunity to spread awareness about the organization's activities. Web jacking serves political, social, or economic interests.

Denial of Service Attack

DoS or Denial of service is where the attacker floods a network with unnecessary traffic so that a website or domain becomes inaccessible.

Email Spoofing

Hackers manipulate headers of an email, so it does not show the source. This is done to trick the recipient into giving away sensitive information.

Salami Attack

A salami attack is marginal in nature and can go unnoticed for a long period. An example of a salami attack is when the attacker targets bank accounts of multiple users to withdraw 1 cent every day from each account. The users would not notice it, but 1 cent from multiple users' bank account over many days can amount to a lot of money in a few months or years. Banks now monitor any unusual withdrawals immediately and notify the owner about the transaction.

Data Diddling

The act of manipulating data before it is entered into a computer

system is data diddling. For example, an attacker can change the salary they are due to receive from the company on the day of payroll calculation. They can receive a higher salary from the company, but the company's report shows they were paid the amount they were due.

Logic Bombs

Malicious code injected into genuine software is known as a logic bomb. The malicious code is triggered by an action the user performs. When the malicious code is triggered, it can destroy information on the system or destabilize the system.

Chapter Three: Recognizing and Countering a Phishing Attack

What is Phishing?

Using a phishing attack, an attacker tries to get sensitive information, such as user accounts, bank and credit card details, and other important credentials. As mentioned earlier, the attacker may use electronic media, such as text messages or emails, and pose as a genuine user or organization to trick the end user into clicking a link or downloading an attachment. Since the email looks like it has come from a legitimate source, the user may divulge some sensitive information.

Phishing attacks have been pain points for both individual users and organizations. Any kind of information gained from an individual or organization is valuable as it may help the attacker gain monetary benefits or attack the network used by the organization. Additionally, some states or nations may use phishing attacks to obtain the sensitivity of other countries.

Methods used for Phishing

The most common method used for phishing is an email where the attacker tries to obtain sensitive information by coercing users to access and interact with malicious websites. Here are some other methods that hackers use to perform this attack.

● An attacker may manipulate links in emails sent to you. They do this by changing the URL slightly, so the user cannot differentiate between the malicious link and the actual website. For instance, most web-based applications offer a “Forgot Password” feature. When you click on the button, the website sends you an email to reset the password. If the hacker manages to reroute the email, they can send you a different link where you enter your username and the answer to a security question. The hacker can then use that information to access your account.

● Some hackers also use website forgery as a means of phishing. This is a process where the attacker uses JavaScript commands to develop a fake website that looks genuine. This makes it easier to

track the user.

- Attackers also make use of a technique known as covert redirection. In this process, they infect genuine websites to throw pop-ups. A user clicks on links in the pop-up that redirect him or her conveniently to the attacker's website.
- Attackers can deploy malware and ransomware to a user's system or network through infected.EXE attachments, PDFs, and Microsoft Office attachments.
- Attackers can also perform phishing attacks through other media, such as text messages, telephone calls, and social media.

Common Ways to Tackle Phishing Attacks

This section lists the different methods to protect your system and network from different types of phishing attacks. Some of the common methods used are:

- Malware Scanners
- Auto updates
- Multi-factor Authentication
- System or data backups

This will be detailed later in the book. In addition to the methods mentioned above, there are other techniques you can use to protect your system and network from phishing attacks.

Types of Phishing and How to Protect Yourself against Them

Deceptive Phishing

Deceptive phishing is the most common type of phishing attack. The attacker employs deceptive phishing by imitating a genuine email sender or organization to trick the user into giving out personal information or login details. This is done by using emails. The email content creates a sense of urgency, causing the user to panic and do exactly what the attacker intended them to do.

For instance, the attacker may send an email to one or more users telling them their credit will be deactivated if they do not make the payment using the link in the email body. When the user clicks on the link, they are redirected to the attacker's website, which is a replica of the bank or payment gateway. The user then

enters their credit card details, including the expiry date and security code. The attacker now has all the necessary information to make fraudulent transactions on the user's credit card.

The success of a deceptive phishing attack depends on how closely the phishing email resembles that of the actual organization's email. Users need to go through the URLs of both the email address and the links in the email body to protect themselves before they click the link or download any attachments. Other common indications of a deceptive phishing email include spelling and grammar errors, and generic salutations.

Spear Phishing

Not all phishing attacks employ "spray and pray" techniques and are without personalization. Many phishing attacks depend heavily on personalized emails and messages, and this is where spear phishing comes into the picture.

Spear phishing attacks ensure that the name, address, phone number, company, position, job profile, etc., are included in the email body so that the recipient is convinced that they have a relationship with the sender. The objective of spear phishing is ultimately the same as deceptive phishing—to trick the user into clicking on a malicious link or downloading a malicious attachment. The attacker can use either of the two means to obtain sensitive information. Much effort is needed to create a spear phishing email since the attacker must obtain some personal information of the target. Therefore, social websites like LinkedIn are commonplace for spear phishing attackers from where they try to retrieve as much personal information of a target as possible.

The organization must conduct specific training regularly to ensure their users do not respond to such emails. Businesses should also invest in technologies that scan incoming emails for known malware.

Whaling Attack

Spear phishing can be employed to attack everyone in an organization, including top executives, and this is a whaling attack. The attacker targets whales or high-level executives to steal their information and login credentials.

A successful whaling attack can lead to CEO Fraud. As the name suggests, CEO fraud is where the attacker uses the CEO's email to approve large financial transactions once they receive their bank

information. Another application of whaling is where attackers use the executive's email account to request other employees' personal information, so they can file fake tax returns using the employees' details. They can also choose to sell this information online.

Most attackers get away with whaling attacks since the top-level management in most organizations is ignorant about information security. Whaling can be avoided simply by making security awareness training mandatory for all employees, including top-level management. Businesses should also implement two-factor authentication or multi-factor authentication processes for financial transactions to ensure they cannot be completed through email alone.

Vishing

The previous phishing attacks depend exclusively on email as a medium for the attack. Email undoubtedly is the most popular phishing medium, but attackers also resort to other media at times.

Vishing is a phishing technique that uses phone calls to scam users. When the telephone gained popularity, people only communicated using it. However, with today's advancement in technology, calls can be made using the Voice over Internet Protocol VoIP, where an attacker can imitate genuine organizations to steal information from a user.

There are various forms of vishing. For instance, in September 2019, attackers launched a vishing attack on the MPs and other parliamentary staff in the United Kingdom to steal their passwords. In the same year, there was another vishing attack where the attackers pretended to be the top management of a German organization and coerced their UK subsidiary to give away information to steal money worth USD 243,000.

The simplest way to avoid vishing is never to answer calls from unknown numbers, use an app for caller identification, and never divulge personal information over the phone to anyone.

Smishing

Vishing is not the only method where attackers use a phone to implement a phishing attack. Attackers also use text messages to perform a hack, and this form of hacking is known as smishing. The message contains a link or a phone number that the receiver must click or call on.

Smishing attackers also pretend to be genuine entities. In

February 2019, Nokia sent a warning to everyone in the world where smishers were pretending to be Nokia and sending out messages to users saying they had won money or a vehicle. When the hackers initiated the scam, they would ask users to send them a nominal amount as the registration fee to claim the vehicle they won.

In the same year, there was a story of a woman who was a victim of a smishing attack. The woman had cancer, and the smishers tricked her into believing that they were from the government, offering her a grant to pay for her treatment. The attackers asked her to make a nominal down payment and pay taxes in order to be eligible for the grant.

Again, the simplest way to avoid a smishing attack is to look at the number that is messaging you and then decide to do something about it. Alternatively, it is also a good idea to call the company cited in the message and cross-check if they actually sent any such message.

Pharming

Attackers are aware that users are getting wiser and being trained against common phishing scams. Therefore, most attackers no longer use methods where they need to use bait to obtain sensitive information. They now use pharming, where they take advantage of cache poisoning in the Domain Name System. Domain Name System, or DNS in short, is a naming system used by the Internet to convert strings to IP addresses such as google.com to a numeric IP to land the user on the website for Google.com.

When an attacker employs the DNS cache poisoning technique, they attack a DNS server and change the IP of a certain website to their own IP. This means that the attacker can redirect a user to their website instead of the genuine one. This happens even if the user enters the correct website name.

Pharming attacks can be avoided by training users and employees to enter sensitive information only on websites secured by a digital certificate and resolved on the HTTPS protocol. A business should also install antivirus and anti-malware solutions on all official devices and update virus signatures regularly. Internet Service Providers should also take proactive measures to secure their networks.

Identifying a Phishing Email

This section will go through an example, so you can understand what a phishing email looks like, how to identify it, and what measures can be taken to avoid being tricked by such emails.

What is Email Spoofing?

Email Spoofing is a methodology under the umbrella of Email Phishing where an attacker manipulates the headers of an email to make the source of the email look genuine even when it is coming from an illegitimate source, like the attacker's system. Attackers are aware that users trust an email as long as the sender's email address resembles an address they have seen before. The motive of email spoofing is to trick the user into believing the email they have received is important, and the sender is genuinely requesting information.

Identifying a Spoofed Email

There are two ways to identify a spoofed email:

If the subject line is similar to any of the examples given below, the email is not valid:

- Your email account abc@example.com is hacked
- Urgent: Change your email account's password right away
- Your bank account is hacked
- Security Alert: Save your email accounts

If the email content asks for the following information, it is a spoofed email:

- Personal details or your bank account details
- Requesting you to send money to a particular account
- Password reset link even though you did not request a password change
- Other unknown links to verify details

How do you confirm that the email is indeed a spoofed or spam email from the email headers?

You can determine the authenticity of the email by looking for either of the following parameters within the email source:

Received-SPF

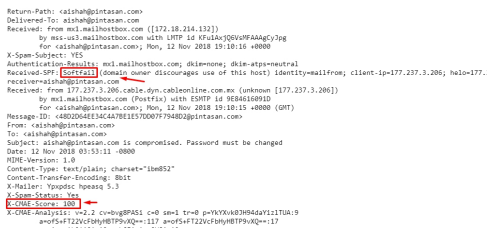
SPF is an implementation of authorization through a TXT DNS record in the domain's DNS zone to authorize emails to be sent only from authorized sources. The syntax contains an IP address added by the domain owner, which means the SPF check in the email

headers will pass only if the email originated from that IP. If the email originated from any other IP, the SPF check fails, and the emails are redirected to the spam folder of the recipient.

X-CMAE-Score – 100

This is the spam score of the email. The recipient email server has certain spam checks in place based on what spam score it assigns to the email, 100 being the highest.

This is how the header of an email looks like. You can access the header by viewing the original source of an email in the email provider's interface, like gmail.com.



The most frequently asked questions when a user receives such an email are:

Is my account compromised if I receive such an email?

No, your email account is not compromised in any way. The email received is either spam or a spoofed email.

Why isn't the server classifying such emails as SPAM?

Most servers have stringent email checks in place that classify these emails as SPAM. These emails automatically move to the Spam folder of the user's email, but there are times when these checks can skip an email.

Can I completely avoid receiving a spoofed email?

No, in every case, the spammer may use a different subject and a different body, so creating a global filter won't help. This filter may block legitimate emails.

Reference Email: (Template Used)

Hi, stranger!

I hacked your device because I sent you this message from your account. If you have already changed your password, my malware will intercept it every time. You may not know me, and you are most likely wondering why you are receiving this email, right?

In fact, I posted a malicious program on adults (pornography) of

some websites, and you know that you visited these websites to enjoy (you know what I mean). While you were watching video clips, my Trojan started working as an RDP (remote desktop) with a keylogger that gave me access to your screen as well as a webcam.

Immediately after this, my program gathered all your contacts from messenger, social networks, and also by e-mail. What I've done? I made a double-screen video. The first part shows the video you watched (you have good taste, yes . . . but strange for other normal people and me), and the second part shows the recording of your webcam.

What should you do?

Well, I think $608 (USD dollars) is a fair price for our little secret. You will make a Bitcoin payment (if you don't know, look for "how to buy Bitcoins" on Google).

BTC Address: 1GjZSJnpU4AfTS8vmre6rx7eQgeMUq8VYr (This is CASE sensitive, please copy and paste it)

Remarks: You have two days (48 hours) to pay. (I have a special code, and at the moment, I know that you have read this email). If I don't get Bitcoins, I will send your video to all your contacts, including family members, colleagues, etc.

However, if I am paid, I will immediately destroy the video, and my Trojan will destroy itself.

If you want to get proof, answer, "Yes!" and resend this letter to yourself. And I will definitely send your video to any twelve contacts. This is a non-negotiable offer, so please do not waste my personal and other people's time by replying to this email. Bye! Please investigate the issue and get back to me.

The attacker has sent this email by spoofing the user's own email address, making them believe they have access to the user's email account. If you look at the content, the attacker is trying to convince an innocent user by saying they have access to the user's computer even when they do not. The user, if not careful, will believe the attacker and give in to their requests. However, examining the headers of the email will help the user understand if this attacker actually has access to their email or is just bluffing.

Most types of phishing scenarios have been covered in this chapter, with an example of email phishing. You can use this as a guide to help you identify and avoid any phishing attacks. This does not guarantee that you can recognize every phishing attempt.

Attackers also do their research and learn more about user behavior, and they use this information to improve their attacks. Keeping this in mind, users and organizations should train themselves to learn more about any new phishing techniques hackers use today.

Chapter Four: How to Identify and Remove Malware

Malware is an umbrella term for different malicious software, such as spyware, ransomware, and viruses. Malware is a code developed by attackers to attack a system and associated data or access a third-party network. The medium used to deploy malware is most commonly an email. The email contains links or attachments that, when clicked or downloaded, result in the execution of the malware code.

Malware appeared in the late 1970s, with the introduction of the Creeper virus, which threatened individual users and organizations. Since then, the world has seen thousands of malware variants, all having the same intent—disruption and destruction of services.

The malware contains payloads that are deployed on target systems in various ways. An attacker's motives range from demanding money to stealing information, and they are beginning to get smarter with their attack techniques. Here are the different types of malware present today.

Types of Malware

Some of these terms have already been briefly discussed in the cybersecurity terminology section in Chapter One. In this section, you will understand them in more detail.

Viruses

Virus is a generic term used by regular computer users and the media for any malware that makes the headlines. However, it is unfair to say that all malware is a virus. A computer virus attaches to files on your system or on pointers to those files and gets triggered when the user executes the files. For example, a user may be executing a normal PDF document, and the virus would have leached onto it via embedded code.

The digital domain does not commonly have any pure viruses today as they make up for less than ten percent of malicious software. This is a good thing. The virus is the only subgenre of

malware that sits on one file and then spreads to another file. Given this nature, it becomes a difficult task to clean viruses as they can keep spreading. Cleaning up viruses has always been complicated, and even the best antivirus solutions struggle with it. Most antivirus solutions are only capable of detecting and quarantining infected files. They cannot clean them and, therefore, just end up deleting these files as a last resort. One may argue what the harm is in deleting files, but if these files are essential for your application or web application to function, their deletion will lead to malfunction of your application or website.

Worms

The history of the existence of worms predates viruses. They have been present ever since the development of mainframes. They became popular in the 1990s with the introduction of email, and security experts were frustrated with worms arriving as email attachments. One employee would open an email with a worm, and the entire organization would be infected in a short period.

What distinguishes a worm from a virus is that a worm is self-replicating. For instance, the Iloveyou worm, on the days of its inception, took over the world by affecting emails, phone systems, television networks, etc. Other popular worms, like MS Blaster and SQL Slammer, also ensured that they would be remembered forever in computer security history.

A worm is extremely dangerous because it can spread like wildfire without any user interaction. Contrary to this, viruses need a human to trigger them and then infect other files. Worms can just depend on files and processes in the system to execute.

For instance, the SQL Slammer still holds the record to date for exploiting a vulnerability in Microsoft SQL, to create buffer overflows on every SQL server with Internet connectivity within ten minutes.

Trojans

Attackers have moved from worms to Trojans as a weapon for implementing attacks. Trojans pretend to look like genuine programs or files but have malicious code embedded in them. Trojans were present in the digital world even before viruses and are the most popular malware amongst cybercriminals today.

Like viruses, even Trojans need user interaction to be executed. Trojan use emails or malicious websites as a medium to arrive at a

target system. The most common and popular type of Trojan is a fake antivirus. You may have seen pop-ups while visiting certain websites that say your computer is infected and asks you to download software to clean the virus. You may believe that it is true and take the bait and end up downloading and installing a Trojan instead. The Trojan then takes control of your system.

It is difficult to defend yourself against a Trojan for two reasons.

1. Trojans are easy to code, and cybercriminal groups have even developed Trojan building kits today.

2. Trojans are deployed onto a system by tricking users, and therefore, they conveniently dodge traditional defenses like a firewall.

There are literally millions of Trojans that are developed every month. Antivirus developers try their best to counter Trojans, but the signatures are too many to keep track of.

Hybrid Malware

The malware present today is a hybrid combination of malicious software, Trojans, and even viruses. The malware may look like a Trojan in the beginning, but its execution will end up attacking all users on the network, a nature exhibited by worms.

Malware programs today are considered to be stealth programs or rootkits. This means that the main objective of malware today is to take control of the computer's operating system and manipulate it in such a way that even anti-malware programs cannot detect it. The only way to get rid of such malware is to disconnect the memory component that has control of the system.

Another hybrid combination of Trojans and worms are bots that exploit one system and try to add it to an attack toward a larger infrastructure. Bots place themselves on individual computer systems and then receive instructions from botmasters, which are command and control servers for the bot network. Bot networks known as botnets can infest a few hundred computers to a network of thousands of servers over the Internet, controlled by a single botmaster. Botmasters often rent these botnets out to other criminals who use them for their specific needs.

Ransomware

Ransomware is malware through which attackers encrypt all your data and demand a ransom to decrypt it. Attackers initially used to target individual users with ransomware but realized the

monetary benefits of targeting bigger institutions, such as banks, hospitals, etc. Ransomware will be discussed in depth later.

Fileless Malware

This is not really a different type of malware but has made it as a classification based on the way malware is used to exploit a user. Traditional malware infects systems by taking control of the file system. On the other hand, fileless malware does not touch the file system but spreads within system memory or employs other non-file components such as APIs, scheduled tasks, and registry keys.

Fileless malware exploits a program running in the system to become its sub-process. Or it uses system tools such as the PowerShell in Microsoft Windows-based operating systems. Attackers have started using fileless malware because they are difficult to detect.

For instance, Operation Cobalt Kitty is a fileless malware that became popular for infecting PowerShells and attacking Asian companies for six months. The malware was deployed onto target systems by using spear phishing emails.

Adware

If you have come across malware only in the form of adware, consider yourself lucky. Adware infects a computer and just keeps popping up unwanted ads. The most common ads that appear through adware redirect users to websites containing promotions for other products. Adware is potentially harmless but can get very annoying.

Malvertising

Do not confuse this with adware, but malvertising makes use of genuine ads to deliver malicious files to a target system. For example, an attacker might pay a website to place a malicious ad on their web page. A user clicking on this ad will be redirected to the attacker's website or will instantly download malware onto the user's system. Often, malware in the ads executes without any user interaction, a technique called drive-by-download.

There have been instances when attackers hacked into big ad engines like Yahoo to deploy malware through their ads into bigger websites, such as Spotify, New York Times, The London Stock Exchange, etc.

Attackers use malvertising to make money. They deploy malware

through ads that are capable of crypto mining and ransomware infections.

Spyware

Spyware is a type of malware used by attackers to spy on people's activities. It is mostly used by partners in a relationship to spy on each other, but attackers also use spyware to understand a target's activity and log their keystrokes.

A regular scanner can detect spyware and help you uninstall it.

Virus Vs. Malware

It is a common practice for people today to use malware and viruses interchangeably, but they are not the same. The difference is that malware is the parent term, and a virus can be a kind of malware. In simple terms, a virus can be malware, but all malware is not a virus.

If represented as a Venn diagram, it would look something like this. A virus is a subset of malware, which is a subset of a threat.

Knowing this, you may now have the following questions.

Why is there confusion if they are different?

Entrenched name recognition is to be blamed for the confusion between a virus and malware. Once a word is put in someone's head, it tends to stay there. For instance, Xerox is a company that deals largely in photocopy machines. However, since the very beginning, a photocopy was known as a xerox, and the term has stuck.

How can you tell if your system has a virus or malware?

A virus will mostly infect one file and replicate itself onto other files. That is the job of a virus if it is purely a virus. However, if the virus was deployed to be malware, the most common indication will be your system slowing down.

Do you need both antivirus and anti-malware?

Today, antivirus and anti-malware solutions are the same thing. No provider will give you a solution that only checks for viruses and leaves out scanning other malware like worms, Trojans, ransomware, etc.

A good security solution will scan local files on the system and also monitor your online activity via email and surfing websites. If you visit a malicious website, your security solution will not even allow it to load in the browser.

Protecting Yourself from Malware

If you feel that your system is infected, follow the steps given below immediately.

Install/Update your Antivirus

If you do not have an antivirus solution, purchase one, and install it immediately. It is a small price to pay for your system's health and the important data it contains. You can trust providers such as Norton Security, Kaspersky, McAfee, and Avast, among many others. Most of these solutions are rated 4.5 stars. Run a deep scan once you have installed the antivirus and let it run even if it takes a lot of time. The only problem is that the malware is very advanced; it knows how to deactivate the antivirus.

If you already have an antivirus solution and it has failed to detect the malware, it mostly means that you have not updated its signatures. The job is not over by just installing an antivirus solution. New malware is developed every day, and therefore, you need to update your antivirus signatures so that they can detect this new malware. You are opening your system to new malware even if your antivirus is a single day out of the update.

System Restore

Most operating systems, such as Microsoft Windows, have a feature called system restore. This basically stores an image of your entire system at regular intervals. This means that if your system contracted malware today, and there is a system restore point available for yesterday, you could restore your system to how it was yesterday, which will remove the malware. However, sometimes malware code is written so that it won't let you run the system restore. In such cases, you may need to reboot your system to enable safe mode and then try to run a system restore.

Disconnect from the Internet

If there is malware that is being used to steal information from your computer, it means that someone is remotely controlling it through the Internet. The first step to deal with this is disconnecting the Internet completely. Plug out the Ethernet cable, disable Wi-Fi, and even shut down the router if needed.

You may argue that your antivirus will not update if you have disconnected the Internet, but you can install antivirus through an offline solution. At least you will be at peace that the attacker no longer has access to your information.

Get a Portable Antivirus Solution

If everything is failing, and you are not even allowed to install antivirus, it means the malware has taken control of the operating system. You need to find a way to take control without having to deal with the operating system.

In such cases, you can use portable antivirus solutions that can be loaded on to a USB drive. Some of these are ClamWin, Kaspersky Security Scan, McAfee Stinger, and Microsoft Safety Scanner. You can, in fact, have all of these on a USB drive and run individual scans without causing any conflict.

Chapter Five: Recovering from Ransomware

In recent years, you may have heard of the term Ransomware in your office or on the news. What is the fuss all about? Perhaps you received a pop-up on your computer screen saying your system is infected by ransomware. This chapter sheds light on what ransomware is, its types, a little history, and what you should do to protect your systems.

Defining Ransomware

Ransomware is the conjunction of the words ransom and malware. It is malware that infects your computer and encrypts all the data on it, restricting you from accessing it. It then demands a ransom payment if you wish to access all the data again. Ransomware first featured in the 1980s and payments were demanded via snail mail. Today, ransomware is much more evolved, and hackers demand payments via credit cards or cryptocurrency.

How Can You Get Infected?

Attackers can use ransomware in different ways to infect your system. A common way to do this is to fill your inbox or desktop with malicious spam, also known as malspam, where the medium used to deliver spam is an email. The email contains malicious attachments, such as word documents or PDF files, or even hyperlinks to third party websites.

The malspam method employs social engineering tactics to make people believe the email and its attachments are genuine. The hacker does this by making them appear as if they come from a trusted source. Attackers also use social engineering in ransomware attacks where they pose to be the FBI to scare users and make them pay to access their files.

Malvertising is another popular ransomware infection method that peaked around 2016. As the name suggests, malvertising employs the method of online advertising to spread ransomware. This type of ransomware did not interact too much with the users. Even today, you may come across websites filled with ads that redirect you to third-party websites without your permission. These third-party websites are kept to log all your activities and

information. They then deploy malware on your computer. Most often, this malware turns out to be ransomware. Malvertising makes use of a technology called iframe that has malware hidden in invisible HTML elements. This iframe will redirect you to a malicious website, and the malware will be conveniently deployed to your computer from this website through an exploit kit. This process is called a drive-by-download process as everything happens without the user knowing what is happening.

Types of Ransomware

Ransomware is classified into three types based on their severity.

Scareware

Scareware is ransomware used to carry out tech support scams on old security software. You may receive pop-ups on your device asking you to download some information from a website. The pop-up may say there is a virus on your system, so you do exactly what the pop-up says, and find that your system is infected with a virus. If you ignore the message, several other pop-ups follow. However, your files will still be safe.

If you have an anti-malware solution from a genuine provider, run it and see if there is some virus on your system. If you do not have an anti-malware solution on your computer, download one immediately before you resort to downloading anything from the link they share with you.

In this case, the attacker is bluffing and trying to scare you in the hopes you fall for the trap.

Screen Lockers

This type of ransomware is an orange-level or medium type of ransomware. As the name suggests, this form of ransomware locks the target user out of their system. When the user tries to unlock the system, they can only see the US Department of Justice's logo or the FBI's logo. The message on the screen may say that they were caught doing something illegal, and therefore, must pay a fine.

Firstly, it is important to know that any law institution will not lock you out of your computer or ask for a payment. If the FBI suspects you, they will contact you directly via legal channels.

If you find yourself in a situation where your screen is locked and you cannot enter the system without making a payment, your system has been hacked.

Encryption Ransomware

This is the most dangerous form of ransomware because an attacker deploys encryption ransomware onto the victim's system and encrypts all the files so the victim cannot access them. They then demand a payment to decrypt all the files to the original state again. It is considered the most threatening form of ransomware due to how difficult it is to decrypt files once encrypted—since no software can decrypt all forms of encryption. It is best to assume those files are lost unless you want to pay the ransom. There is no guarantee that you will get your files even after payment.

Ransomware History

The first occurrence of ransomware was in the 1980s, and it was called AIDS or PC Cyborg. This ransomware encrypted all files of a user present in the C: directory every time the user restarted the system. The ransomware collected all the files after 90 such reboots and then would send the user an email asking them to renew the license to the operating system. They may ask them to pay $189 to PC Cyborg Corporation. It was a very simple encryption technology, and therefore, was easy to reverse. Thus, users from the computer science industry knew how to reverse it, but it majorly impacted common people who were not so tech savvy.

Over the next ten years, a few other variants appeared, but dangerous ransomware did not make a debut until 2004. This was the year when GpCode took advantage of weak RSA encryption to encrypt user files.

The next big ransomware showed up in 2007 when WinLock was introduced. Unlike other ransomware, WinLock did not encrypt user files but locked a user out of their system. It also showed pornographic images on the user screen. The attackers would then demand payment via SMS to grant the users access to their systems.

Ransomware evolved in 2012 with the development of the ransom family called Reveton. This gave birth to another type of ransomware known as law enforcement ransomware. Attackers locked people out of their systems and left the FBI's official logo or any other law enforcement agency's on the lock screen. There would be a statement saying you committed a crime, such as downloading pirated content, hacking, or watching pornographic content on the screen. They would also imply to the target that they must pay a fine ranging from $100 to $3,000 using a prepaid cash

card.

Some people did not understand this, and they believed they had broken the law, and therefore, had to pay a fine. This is a social engineering tactic called “implied guilt,” where a user questions his or her actions. They don’t want to be called out publicly for an activity like watching porn, which they believe is a crime, and so prefer paying the ransom to end it immediately.

Encryption ransomware resurfaced in 2013 with CryptoLocker but was far more dangerous. The CryptoLocker ransomware employed military level encryption, and the hacker would store the decryption key on a remote server. There was no way for users to retrieve their files without paying a ransom. This type of ransomware is even present today, and some cyberattackers are still making money off it. The recent ransomware outbreaks such as Petya and WannaCry in 2017 also made use of similar encryption techniques.

As 2018 came to an end, another ransomware called Ryuk was developed by skilled hackers, and this created trouble for news publications in America, especially the Onslow Water and Sewer Authority in North Carolina. This ransomware attack was planned, so the attackers could first infect the target systems using information-stealing Trojans called TrickBot and Emotet. They would then use this information to install Ryuk and other ransomware in the system. Cybersecurity experts believe that hackers used TrickBot and Emotet to target high-profile business people. These Trojans infected random systems and deployed Ryuk once they identified that the target system belonged to a high-profile businessman, and the attacker could make a lot of money.

Coming to the present day, a new type of ransomware called Sodinokibi, known to be an evolution of GandCrab, has been making news. The attackers use managed service providers to spread this ransomware. In August 2019, several dental care centers lost large volumes of data, and hospitals were unable to obtain records of their patients. The attackers used a compromised manager service provider to upstream the ransomware to 400 dental care centers.

Who are Targets of a Ransomware Attack?

When ransomware was invented, the primary victims of it were

individuals who were regular computer users. Attackers realized later that ransomware had more potential, especially when they began to target businesses. When an attacker used ransomware to attack a business, they ensured they could stop the production, and create a loss in data and revenue. Attackers soon realized that attacking a business would fetch more money than attacking regular users. At the end of 2016, statistics showed that ransomware was detected on roughly thirteen percent of global businesses and only two percent of regular users' computers. By 2017, almost 35 percent of small and medium-sized businesses were already victims of ransomware.

Geographically speaking, attackers deploy ransomware mostly on western markets, and the United Kingdom, the United States, and Canada are their biggest targets. Research shows that ransomware attackers always choose businesses and countries with more money. This means they look for regions where computer and Internet adoption rates are high, and the region is wealthy. It is believed that they will target the Asian and South American markets very soon, too, as these regions are picking up in terms of economic growth.

What to Do If You Are Infected

The thumb rule to follow if you are a victim of ransomware is never to pay the ransom. Even the FBI encourages you not to pay. If you pay the ransom, you end up doing what the attacker wants you to do. Therefore, you may encourage them to continue plotting ransomware attacks for the future. There is a small probability that you may get some of your files back using free file decryption software.

However, there are only some ransomware attacks that these tools can reverse or prevent. Also, if a decryptor is available, you must ensure it helps to protect the system from ransomware already present on your system. It is advisable not to run any decryption software without knowledge as you may just end up encrypting your files even more. It is also important to look closely at the ransom message that appears or seek help from an IT security consultant.

Other known methods for cleaning ransomware include anti-ransomware products to scan your system and remove the infection. These solutions may not help you retrieve your files but clean your

system. In cases of a screen locker, try to restore the system to a previous health point or try running a scan from a bootable USB drive or DVD.

If you want to defeat a ransomware attack while it is in progress, you must stay alert at all times. If you notice slowness in your system for no reason, it is best to restart the system and disconnect the Internet. This ensures that the malware is inactive when you boot the system. It also cannot send or receive instructions from the commanding server or attacker. This means that since the attacker has not completed the activity, they cannot have encrypted all files in the system, and thus, cannot demand money. At this point, you must install an anti-malware solution and run a complete scan of your system.

How Do You Protect Yourself from Ransomware?

Most security experts worldwide have one thing to say when it comes to protecting your system from ransomware—they ask you to prevent the attack from happening.

There are a few methods to tackle a ransomware infection, but there is no evidence that they work. Most of them also require high-level technical expertise, and an average user may not be ready for such tools. Therefore, it is suggested that you follow the remedies below.

The first step is to purchase a paid anti-malware solution that provides real-time protection. This solution can also detect attacks from advanced ransomware. The solution should also be capable of protecting vulnerable files and software while also blocking ransomware from encrypting any files. One such solution is the paid version of Malwarebytes, which protected users from all types of major ransomware attacks in 2017.

The next step takes time and effort. You must regularly create backups of your data and store it on external media. Experts recommend that you store backups on a cloud-based solution that is protected via encryption and multiple-factor authorization. Another option is to store the backups on external media like USB drives or hard disks. However, ensure you disconnect them after you take the backup. Otherwise, there is high chance ransomware may infect these external devices too.

The next step is to ensure your operating system and other software is up to date. The popular WannaCry ransomware

exploited a vulnerability in the Microsoft operating system. Microsoft released an update in March 2017 to patch the vulnerability, but most people ignored this update and did not download it. This left their systems open to an attack. It is understood that manually updating the operating system and other software is difficult, and therefore, it is best to enable automatic updates for the operating system and other software.

Finally, it is best to stay informed. The most common technique used by an attacker to deploy ransomware is social engineering. Educate yourself and your employees about how to detect malicious websites, malspam, and other harmful media. Always trust your instincts. If something seems harmful, it probably is.

How Does Ransomware Affect a Business?

Many businesses have been hit hard in the past few years by different types of ransomware, such as WannaCry, SamSam, GandCrab, and NotPetya. The number of ransomware attacks on businesses increased by 88 percent in the second half of 2018 as attackers stopped attacks on computers and normal users' systems. Attackers understood that they could earn more when they attack big businesses, such as government agencies, hospitals, and other commercial institutions. The average damage done by ransomware, including data loss, reparations, fines, and ransom payments, comes to about $4 million.

The latest ransomware attacks were identified as GandCrab attacks. GandCrab made its first appearance in January 2018 and has since been evolving to make the encryption stronger, empowering attackers to attack high-profile organizations. Reports suggest that GandCrab has managed to cause damages worth $300 million in ransoms, most of which have already been paid. The range of individual ransoms is between $600 and $700,000.

In March 2018, another ransomware attack was initiated using SamSam ransomware. This attack was launched on the city servers in Atlanta, which infected essential city services, such as police record systems, and revenue collection systems were infected. SamSam caused $2.6 million in damages to Atlanta.

Chapter Six: How to Spot and Stop a Social Engineering Attack

Social Engineering is the process of manipulating or tricking people into giving you the information you need about them. Cybercriminals are looking for all kinds of information, but most commonly, they employ social engineering to coax you into disclosing your bank information, login credentials to various applications, or passwords to access your computer. They may use this information to transfer funds from your accounts to theirs or install malware on your system.

Cybercriminals use social engineering because they know it is easier to win a person's trust than hack software. For instance, they can use simple conversations to manipulate any victim to give you their password. They do not try to hack the system using a password or any other technical process. They may attack the system if the user has a weak password.

The basic principle of security is to know who and what to trust. You must know when to trust a person and be alert when you communicate with them, especially online, since you cannot see them. This holds true for trusting applications too. You must know whether an application you download and install on your system or website is genuine and won't harm you.

Any security professional will tell businesses that the weakest point in a security chain is a user who accepts and trusts another user at face value. In simple words, it does not matter if you have top-notch security for your house with multiple locks, guard dogs, floodlights, alarm systems, barbed wire, fences, etc., if you let a stranger enter your home simply because they claim to be a plumber without doing any checks. In a case like this, you empowered the threat to enter your house.

Social Engineering Methodologies

There are three types of methodologies employed for social engineering:

- Phishing
- Vishing

● Impersonation

Phishing and Vishing were discussed in Chapter Three; however, Impersonation is when an attacker pretends to be someone you already know and tricks you into giving them access to your computer, network, etc. An attacker does a lot of research before using the impersonation technique to hack your accounts and systems. Attackers stalk people on social media and company websites and gather information about the victim's friends and colleagues. They may also eavesdrop on your conversations and try to sniff around documents you have trashed.

Here are a few statistics to help you understand these social engineering methods concerning their application in the real world.

Phishing

● Seventy-seven percent of the social engineering attacks carried are implemented through phishing.

● Roughly 40 million people report phishing attacks every year.

● Eighty-eight percent of all reported phishing was via links clicked within emails.

● Ninety percent of all email traffic in the world is full of spam and viruses.

Vishing

● Sixty percent of adults in the USA were victims of vishing in 2012.

● 2.4 million customers were targets of phone fraud in the year 2012.

● 2.3 million customers were targets of phone fraud in the first half of 2013 itself.

● USD 42,500 was the average loss per customer to a business.

● When a vishing SMS was received, 60 percent of users clicked on the link in the message, twenty-six percent of users tried to call the number, and fourteen percent of users replied to the text.

Impersonation

● 1.8 million people were victims of impersonation in the USA in 2013. Medical identity thefts increased because of websites impersonating medical providers.

● Eighty percent of thefts happened at the workplace that involved bypassing controls.

● Eighty-eight percent of the stolen information was personal

data.

● The average age of a victim of impersonation was 42 years, and the average loss incurred by them was USD 4,200.

Spotting a Social Engineering Attack

What does a social engineering attack usually look like? The following are some common scenarios to understand how social engineering works.

An Email from a Friend

If the attacker manages to hack a user's email password via software or social engineering, the attacker has access to that user's contact list. Given that most users use the same password for numerous web applications, the attacker may gain access to the user's social media and contacts on social media too.

From here on, everything is home territory for the attacker. They can send emails to the user's contacts or instant messages on social media. Most of the messages sent by the attacker have the following features:

● A URL, where the attacker pretends to be a friend and excites you by saying something you can relate to. They may send you a link and ask you to provide some information through that link. Unsuspecting and innocent, because it came from a friend, you click on the link and download malware that infects your computer. The attacker can access your system and perform any action they want. They try to collect information about your contacts and deceive them as they deceived you.

● An image, a video, or music file with a malicious code embedded in the file. You may download the file without hesitation since it's coming from a friend and end up infecting your system with malware. The attacker has access to your computer and the treasure of information that is present on it.

An Email from a Trusted Source

Social engineering is a parent of phishing attacks where attackers imitate a trusted source to trick users into disclosing sensitive information. Reports from Webroot suggest that most attackers impersonate financial institutions. Data from Verizon also suggests that 93 percent of breaches happening today are a result of a

successful social engineering attempt.

Emails from trusted sources may have the following themes:

The emails may ask for urgent help

Some emails may have urgent messages, and the sense of urgency may force you into performing the action in the email. Since you are afraid, you may transfer the funds into the attacker's account.

The email may ask for donations for a cause

The emails may try to exploit your generosity or kindness. The content may say that you need to transfer some funds toward a foundation or cause, but the money goes directly into the attacker's account.

Phishing attempts using a genuine background

An attacker may send you a message or email asking you to send funds. The source of the message or email appears to be from a reputed company, school, or institution.

The email will say there is a problem and ask you to click on a link to rectify it

The URL used to send the email may look genuine, and the body of the email may also use a logo similar to the organization the attacker pretends to be from. It's possible that the attacker sent the email directly from the source website, but uses different means to gain access to that website. Since everything looks legitimate, you may click on the URL, which redirects you to the attacker's website. The attacker may present a form that asks for some information they need to hack into your account. The email also includes a warning that tells you what the consequences might be if you do not click on the URL. This may scare you, and you choose to click the link.

Pretend to be your manager or colleague

The email may have details of a project that you were working on at your office. This will gain your trust. The next part will be related to some kind of payment using a company card you have made in the past. You believe this is legitimate and make the payment.

Tell you that you have won something

You may have received emails from a supposed dead relative, a lottery company, or any other business. Some emails may also say you were the 100th person to have visited the website, and you

won something. The email asks you to provide some sensitive documents, such as your social security number, to prove who you are. These requests should make you suspicious. Do not trust the emails. This type of attack is known as greed phishing. Since you are greedy, you may want to give the attacker the necessary information. As a result, you may provide sensitive information that the attacker can use to empty your bank account.

Baiting

In this social engineering scenario, the attackers know they can bait the user, especially if they want to obtain sensitive information. Such baits are often found on websites offering free movies or music downloads. Attackers may run such scams on malicious websites, social media, and other websites most users stumble upon via search results.

The baiting scheme also shows up on a website that offers to sell an iPhone for only $100 when the actual cost is $1,000. You may be suspicious, but you see that many users have testified that the offer is true. The attacker obviously planned this.

Users who fall for this bait download malware to their computers and this exposes their details and other sensitive information about other users the victim corresponds with. You may even pay them $100 but never receive the promised iPhone in return.

Responding to Questions that You Didn't Ask

At times, attackers may contact you to provide help from a company, while offering benefits. The email ID may resemble one of a renowned company or bank. If you are not a consumer of the product, you will discard the email. However, there is a high chance that you do use the product and were actually planning to contact the company for help. How convenient that the company approached you proactively to extend their help.

For instance, you may not have asked for help regarding an issue with your operating system, but you suddenly see an email from Microsoft. The email offers to fix the issue for free. You respond to them and trust them, opening yourself up to several exploits the attacker has already planned.

The attacker may ask you to validate yourself and ask you to provide the required information to log into the system or application. Other times, they may ask you to run a few commands

on your system to fix the issue. When you let them do this, they access your system.

Distrust Creation

Certain social engineering practices are only implemented to create distrust or conflicts. These are executed by people you know and have a problem with or by people who just enjoy watching the world burn. These attackers will fill your head with wrong impressions of other people you know and then enter as a savior to gain your trust. Such ill practices are also employed by extortionists who want to manipulate you initially and attack you later.

This type of social engineering is initiated by gaining access to one of your accounts. This is achieved by hacking your password, social engineering, or just guessing your password.

The attacker who now has access to your media, like videos and images, may edit them as per their needs and forward it to your contacts to create distrust. They pretend as if the content was forwarded by mistake. The attacker may also use the stolen media content to blackmail the user they hacked or the person they were forwarding the content to.

Social engineering attacks have many variations. The attacker's imagination is the only limit to the number of ways they can exploit someone. A single attack may contain multiple numbers of exploits. The attacker may then sell your information to people who dislike you so you can be exploited further.

How to Avoid Falling for Social Engineering

The shelf life of a social engineering attack is short, and it needs only a few users to fall for it to be successful. However, you can protect yourself against it. It does not even need too much effort as you just need to be aware of your surroundings most of the time.

Tips

Take it Slow

It is a good idea to slow down and give it some thought. Attackers expect you to act urgently without thinking. Most social engineering attacks put you in a situation that looks urgent. This should be your clue to slow down and review the situation properly.

Spend Some Time on Research

Even if you receive an email from a business you believe you

know, go through it thoroughly, not just the body of the email but also the “from” address, the signature, etc. In case you do not recognize the company, do a simple search to see if they really exist.

Don’t Blindly Click on Links

If you receive a link in an email, do not click the link. Make some manual effort to find that website URL through a search and see where the base URL leads you. This way, you are in control of the link and not vice versa.

Be Aware of Email Hacking

Attackers hack email accounts and prey on the contacts of the hacked account based on their trust. Therefore, when you receive an email from someone you know, ask yourself if you were expecting it. Do not click on any link in the mail if you did not expect the mail. It would be a good idea to call the person up and verify if they actually sent you the mail.

Do Not Blindly Download

If you do not know the sender, do not download any attachments in the email.

Know that Lotteries are Fake

No one gives you a whole lot of money for free. So, if you receive an email saying you won something, especially without participating in any kind of competition, it is a scam. A classic example is a scene from *Harry Potter and the Order of the Phoenix* , where Tonks sends a letter to the Dursleys saying they won a competition for the best lawn. She only did this so that the Dursleys did not get in the way when they tried to take Harry to the Burrow. If you receive such an email, it is fake.

Look out for Banking Scams

If the email asks for personal and banking information, it is most likely a scam. Delete this email, also create a filter to discard all future emails from that sender.

Reject Offers for Help

Genuine companies do not proactively contact you and ask you to extend any kind of help. If you receive communication from anyone, especially when you do not initiate the conversation, it may be a scam if they say they can do the following:

1. Offer to help you improve your credit score
2. Fix an application or software on your system

If you receive an email or message from a charity that you do not know, delete it. If you really want to donate to a charity, do some research and donate to a legitimate charity.

Configure Your Spam Filters

Spam filters are a feature to help you classify emails as legitimate or spam. Take some time and play with your spam filters. Set rules to allow only emails you want. There are guides available via your email provider on how to set your spam filters. An investment of time, as low as thirty minutes, will make your “email life” easy forever.

Secure All Your Devices

Install antivirus and anti-malware programs on all your devices, and set the software to run a routine scan. The software must run real-time scans for any incoming email. Ensure that you keep your operating system and other software up to date by enabling automatic updates.

Chapter Seven: Network Security and Protection Techniques

This chapter defines network security and the various processes associated with it. It also looks at the different types of cyberattacks that can affect your business and sheds light on how important it is to secure your network if you want to prevent a catastrophic loss.

Network Security

Network security is an umbrella term covering a variety of processes, technologies, and devices. Network security is the configuration of rules and policies in both hardware and software of any web application or tool to secure the integrity, accessibility, and confidentiality of computer data. This is closely associated with network infrastructure.

Computer data and networks are vulnerable to numerous cyberattacks, and some of these were looked at earlier in the book. Therefore, every business, irrespective of its size, infrastructure, or industry, needs to have network security measures in place.

The network architecture is evolving and becoming more complex every day. The threat environment is also constantly changing with attackers trying to find newer methods to exploit security vulnerabilities in the system. Vulnerabilities exist in various assets of network infrastructure such as data, devices, applications, and users. Given this, there are individual tools available to secure these assets. You can also use these tools to test the applications to ensure the business meets with the regular compliance terms. Network security is of the utmost importance as even a few minutes of downtime can damage the organization's reputation and finances.

How Does the Network Security Function?

Network security across an organization has multiple layers. An attacker can target any layer in the network security model. Therefore, businesses need to define network security models for both hardware and software to tackle the vulnerable areas.

There are three aspects to network security: physical, technical, and administrative.

Physical Network Security

This aspect deals with different types of physical access to network-related devices such as cables, modems, switches, and routers. An organization must ensure only authorized employees, especially those who are a part of the IT or network team, have access to these components. Some common ways in which the business can authorize access is through biometrics, security locks, etc.

Technical Network Security

This aspect deals with the protection of data stored on a network or in transit via the network. The business must include twofold protection to protect data and its associated systems from unauthorized access. Care should also be taken to protect data against malicious activities from internal employees. Internal employees may not do it intentionally, but actions such as using a personal USB drive on company property can be a threat.

Administrative Network Security

This aspect deals with processes and security policies to keep user behavior in control. This includes the authentication of users and the level of access based on the role and designation of the user in the organization. For example, a management bank user does not need technical access to a server or network device.

Top Five Attacks Through a Network that can Affect Your Business

The previous chapter briefly discussed the different types of cyberattacks. This section discusses the top five cyberattacks through a network that can destroy your business.

From scheduling recruitments to customer relationship management, most organizations perform all their tasks online. Automation has reduced human effort and made processes much more efficient and convenient, opening up a window of opportunities for cyberattackers.

A report released by the Center of Strategic and International Studies states that the damage caused by cyberattacks is $600 billion annually. The evolution of technology has led to the development of new methods for attackers to scam a business. Here are the top five cyberattacks that businesses have to deal with.

Advanced Persistent Threat (APT)

This attack's objective is to scan the organization's network and software for vulnerabilities and use those vulnerabilities to steal data. An advanced persistent threat can go undetected for a long period. This attack was first introduced by attackers who wanted to steal government information. Attackers now use this method to steal sensitive information from organizations and claim ransom.

Some indicators to help you determine whether your organization is a victim of an advanced persistent threat are as follows:

- Irregular flow of information – You may notice that the infrastructure is witnessing a sudden increase in inbound or outbound traffic. The flow of data has an irregular pattern, and this can happen between networks, servers, or server to client connections.
- Data bundle usage – An advanced persistent threat collates stolen data before transferring it to the desired computer. If you observe huge volumes of data or compressed data being transferred through your network, it indicates that your network may be infected.
- Increased number of user logins during unexpected hours.
- When you discover backdoor Trojans on the network and associated devices.

Denial of Service Attack (DoS)

A denial of service attack is an attack to prevent access to a genuine user from services, such as bank accounts or email accounts. An attacker attacks the network and server and floods the bandwidth with unnecessary requests. The motive of a Denial of Service attack is not to steal any information but to prevent access to the server or website. The business may incur huge financial losses due to this business.

Assume that a user is trying to access their online bank account. They are unable to do so, despite having good internet connectivity. This indicates that the service is under a DoS attack, and genuine users are blocked from accessing their accounts.

Internet of Things (IoT) Hacking

Internet of Things refers to the devices connected to the Internet either directly or indirectly. When business setup is mentioned, it includes various IoT devices such as thermostats, locks, cameras, etc. An attacker can leverage IoT devices to attack a business. For

instance, there are several IoT devices that businesses forget to update with the security and contain many vulnerabilities. Say an employee connects their smartwatch to a computer at work. If the smartwatch has vulnerabilities, the attacker can exploit those to access the entire infrastructure at work.

It would make sense to uninstall applications on old and unused IoT devices to ensure an attacker cannot take advantage of them.

Structured Query Language (SQL) Injection

Structured Query Language (SQL) Injection is a hacking method discovered years ago but is still effective today. SQL is a language operated on databases and tables programmed in Oracle, MySQL, or Microsoft SQL. The injection affects any application that uses one of these databases, but attackers target websites that employ these databases. Many cases of SQL injection attacks have happened in the past decade.

If an SQL injection attack is successful, the attacker can modify a website's content and retrieve sensitive information, such as user account details. There are two stages to an SQL injection. In the first stage, the attacker observes the target infrastructure and gathers as much knowledge about it as possible. This stage is also known as Reconnaissance. The next stage is the attack stage, where the attacker uses the information collected to break into the target system. In an SQL injection attack, the attacker embeds malicious code in an SQL command to execute their commands.

Man in the Middle

A man in the middle attack is when a third party intercepts the communication between two parties. There are various online channels the attacker can hack to intercept the data, such as websites, social media, emails, messengers, etc. An attacker employing this attack can access your personal and business transactions. A man in the middle attack can stop a message from reaching you or redirect it to someone else.

This is why most communication applications use end-to-end encryption. This means that when you send a message, an algorithm converts plain text into encrypted characters. Once the recipient receives this script, the algorithm on their device decrypts the characters into plain texts again. This way, the information, even if intercepted by someone in the middle, is useless since they do not know how to decrypt it.

These are some of the common attacks businesses fall prey to. The next section looks at different methods you can use to protect your business.

Protecting your Business from a Cyber Attack

Multiple businesses are hit by cyberattacks regularly. Most attackers target those businesses with outdated security features. Here are the various ways through which you can avoid cyberattacks. You can classify these methods into the following types:

- Cybersecurity through hardware
- Cybersecurity through configurations and settings

Cybersecurity through hardware

Security Keys

You may have heard a friend or team member say they have the same password for all their accounts. They may also say their password is their birth year or other simple words. Therefore, without a doubt, the biggest vulnerability in the cybersecurity domain is people.

The tool Yubikeys allows employees to access their accounts without using a password. They also do not have to manage the number of passwords they need to change. Such applications gain a lot of popularity since attackers can use brute force attacks to hack this software. They may use a different combination of letters, numbers, and characters until they find the right password. Businesses should purchase a key for all employees or team members working on sensitive projects. When they do this, they can plug the key into a device and access the required tools, applications, documents, etc.

Many times, an attacker can also trick an employee through phishing to obtain sensitive information. Attacks that lead to maximum damage are results of traps set through social engineering that bypass security flags, and those that do not set off any alarms.

An experienced attacker tries to learn about an employee and get to know intricate details about them. They may obtain information about the people they communicate with regularly. The attacker then disguises themselves as someone the victim knows and sends you an email from an ID similar to the acquaintance's email. The attacker can use these emails to coax you into clicking malicious links to obtain information about the victim.

Yubikeys can help avoid such scenarios and provide additional security features, such as identifying malicious files or links.

VPN Firewalls

You protect your house from thieves by locking the doors and windows. This also helps you safeguard the people at home. You must maintain these locks on your system and network to prevent unauthorized access to your system and network. Senior leadership teams find it surprising when security teams advise them regarding a physical piece of security equipment. Most retaliate with questions like, "Doesn't my computer's built-in firewall protect me?" Yes, but it does not guarantee the security demands of a business.

All communication irrespective of the location can be encrypted using a VPN Firewall. You may be seated in your office or coffee shop and still maintain a secure connection with the Internet. A firewall can maintain secure communication lines with anybody you want to speak with. This helps tackle Remote Desktop brute force attacks, which is the most common type of ransomware attack. A VPN firewall also monitors and logs break-in attempts and provides features to filter employees' access, so they do not access harmful websites.

You can save costs by purchasing a refurbished firewall. However, after the purchase, ensure it is updated with the latest firmware before adding employees to the security policies. Make sure to change the default password of the firewall and configure two-factor authentication for admin access. Nowadays, many firewalls also have a software component for employees to install on their official devices. This process may increase the login process time by a few seconds but ensure better security.

Cybersecurity through Configurations and Settings

Multi-factor Authentication

Most applications offer two-factor authentication, but users are very reluctant to use it. However, this security setting is very effective and much needed today. Here is how it works. The user first logs in to their application using their username and password. After this, the system or application triggers a one-time temporary password, which is sent to another device connected to the application and user, like their smartphone. The user can only access the application once they enter this password.

This cuts out the risks from the probability of an attacker having acquired the user's username and password via methods such as email phishing, malware, or keyloggers. This means the attacker enters your username and password but does not receive the one-time password. This blocks the attacker from the application. The application may send a notification to the user if the attacker tries to hack the application multiple times.

Password Vault

Since users access multiple applications, they must maintain different passwords, but most users use the same password across all applications and devices. They do this so that they do not forget the password. There are password vault applications available today that allow users to store their passwords. That way, you must remember one password for the vault. The password vault has features to create complex passwords, manage, and auto-fill passwords into forms, applications, websites, and system logins. These passwords are random and complex and, therefore, difficult for an attacker to crack.

Auto Updates

As mentioned earlier, most businesses do not update their software and applications, which makes the system and network vulnerable and prone to attacks. Software providers regularly provide patch and software updates to maintain the security of the applications. Whenever a new vulnerability is discovered in the software, vendors create a patch for it to secure the application or software. Therefore, if you do not update the software regularly, you leave the software and application open to any incoming attack. Thus, it is wise to leave all your software on auto-update, so it automatically downloads any patch developed by the vendor to cover the vulnerability.

Full Disk Encryption

Every device part of a business must always be fully encrypted. This means that devices such as mobiles, laptops, hard drives, and network storage must always have an encryption layer. Since most businesses allow employees to work from home, they need to ensure any business devices and data are encrypted. For a low cost, full disk encryption ensures that your data is secure if it is ever stolen.

Malware Scanners

Malware scanners are available at low costs and help to detect any malware threats. The market offers different types of malware scanners, and these are classified based on their functionality and price. As discussed previously, it is important to regularly update your malware scanner to ensure that it detects new vulnerabilities.

IP Address Lockdown

Whenever you work on online applications, it is important to lock the IP addresses down, especially those that access the application. Additionally, you can add two-factor authentication to the application to determine if the user is accessing it. It is better to use a multi-factor authentication before you give the users access to the system.

If you use third-party applications for business purposes, it makes sense to lock the IP addresses that have access to the applications down too. This helps prevent logins from unauthorized IPs, and these IPs belong to attackers from other countries or regions.

System Backups

If you grow crops but do not build a fence around the farm, you allow people to tread on the crops or allow rodents to enter and damage your crops. Similarly, if you have a lot of data, ensure you protect it from attacks and disasters by maintaining a backup. Do this routinely and store the backups on encrypted disks on a different network altogether.

Ensure that backup devices do not operate using the same login credentials as other devices. Create and maintain different passwords for backups so that attackers cannot crack them easily.

Security Training

Create training routines for your teams and teach them the best security practices. A small fifteen-twenty minute training video on subjects such as phishing, spoofing, social engineering, etc. can help employees learn about various types of cyberattacks.

Office 365

If your organization uses Office 365, make sure to check out the Office 365 Secure Score tool. The tool goes through the active settings and configurations to generate a security score for you. Based on the security score, it also gives you suggestions on what you need to do to get a better security score. A better security score indicates that your network and tools are secure.

G-Suite

Many businesses today use G-Suite for email solutions. Google has placed all security measures in place, so it triggers a notification every time it sees unusual activity happening on any of your accounts. For example, log in through a different device or IP address.

Continuous Evolution

It is important for every business, regardless of whether it is a big or small organization, to learn more about the latest cybersecurity practices and newly emerging threats in the information world. Therefore, keep your business and employees updated about security policies, hardware, and software related to your organization.

With all these settings and configurations in place for your business, you will have a better grip on your business infrastructure. That way, you can effectively identify a potential threat when you experience an attack or even before you have been hit.

Some Tips to Maintain Cybersecurity

This section lists some tips to help you maintain cybersecurity in your personal systems. This chapter helps you understand how businesses can maintain network and application security.

Hackers Will Target You

You cannot pretend that a hacker may never attack your system or network. You must remember that every individual is at risk, and the stakes are always high. A hack can harm your personal and financial wellbeing, and ruin your reputation or even the business. Thus, cybersecurity is every individual's responsibility. Follow the tips mentioned in the book and remain vigilant. You must do your part to protect yourself, the business, and others.

Always update the software when you install any software or applications on your system. Always remember that the programs and operating systems are critical to management. You must install the security updates for all software and applications on your device. All you must do is turn on the automatic updates feature in the application, so the updates are automatically downloaded onto your system. Ensure that you update your browsers and any plug-ins.

Be Wary of Phishing Scams

As mentioned earlier, a phishing scam is a threat, and attackers

may use various social engineering techniques to trick you into providing personal and sensitive information that can lead to both personal and financial losses. We also discussed the different types of phishing scams that attackers can perform. Always be suspicious about any email message or phone call where they ask you for too much information. If you are unsure about what to do when you receive phishing emails or messages, refer to the earlier chapters to learn more about them.

Always Maintain Strong Passwords

Every user has many passwords to use and manage, and it is always easy to take some shortcuts. Some users reuse their old passwords, and this is a very unwise thing to do. Password management programs help you maintain unique and distinct passwords across different accounts. If you do not know what type of password to maintain, use these tools to generate strong passwords. These applications may also remind you to update your passwords periodically.

Watch what You Click

Do not visit unknown websites, and never download any software or application from these sources unless you know what they are for. These websites host malware and are automatically installed on your system when you download the application. If you find the link or attachment suspicious or unexpected, you should not click on it.

Do Not Leave Devices Unattended

Technical security is one aspect of your devices, but there is also physical security that you must consider. When you leave your phone, tablet, or laptop in a public space without locking it, anybody can access the information on those devices. If you protect data on an external hard drive or flash drive, you must ensure it is locked and encrypted. Always lock the screen of your desktop or laptop when you do not use it.

You must understand that security experts can only do so much. If you do not help them protect the systems and network, there is no way the business is safe. The attacker can hack the system and obtain the necessary information.

Use the tips mentioned in this chapter to prevent any attacks caused due to your mistakes.

Chapter Eight: Web Application and Smartphone Security

The previous chapter looked at how organizations can secure their systems and networks. But is this enough? Or is there a need for more? Where does the process of security end exactly? Advancement in technology has led to the development of web applications. Today, most businesses have web applications, and many also use the cloud to store data securely. The demands of customers have evolved since the inception of modern Web 2.0 and web applications based on HTML5. Customers want to access data and information whenever they want. All these demands have put pressure on businesses to move their data onto web applications and cloud. For example, banking and shopping operations have moved online. You no longer have to walk into a bank or supermarket physically.

This has made life convenient for customers as they can do things at the comfort of their couch, but it has some drawbacks. This has increased the number of cyberattacks or attempts that hackers make. This led to the introduction of another chapter in the security domain known as Web Application Security.

This chapter looks at web application security, some myths around it, and how businesses can use web application firewalls to keep attackers away from their business.

Web Application Security

A web application firewall or WAF is a security protocol that works at the application level to filter HTTP and HTTPS traffic, thereby providing security from attackers at the application layer. In simple words, if an attacker tries to exploit a known vulnerability in a web application, it can block such attacks and protect the website or application from an attack. However, there are some cons to this process.

Here are some of the drawbacks:

It can only detect known vulnerabilities

A web application firewall has certain rules configured in its settings. It matches the web traffic rules and classifies the

application based on whether the traffic matched with those rules or not. Given this, a web application firewall cannot protect you against newly discovered vulnerability in the web application. However, web application firewalls are effective against denial of service attacks.

It is only as good as its administrator

A web application firewall has rules configured by a user. This means it is only as good as the weakest link in the chain and the user who configured the firewall. It is difficult to determine if there are any issues within the system. Therefore, if an experienced user does not configure the web application, it can be completely useless.

Does not fix security issues in a web application

A web application does not automatically fix its code, and you must understand that. So, if there are loopholes in the application, it can only protect those loopholes from the attacker's eyes based on the configured rules. The code still needs to be fixed by a human developer.

A web application firewall is a normal application and has its vulnerabilities

A web application firewall is a software, like any other application, open to security issues. There are instances where attackers obtained admin access to the web application firewall through vulnerability and turned it off. They also break into the application firewall.

Thus, web application firewalls are an additional layer of security but not the end solution. It is good practice to have a web application firewall (WAF) for an application, but if budget permits, it is always good to apply additional layers of security.

It is important to pay attention to the vulnerabilities in the system or web application and fix them irrespective of the presence of a web application firewall. Businesses should have web application vulnerability testing as an integral part of their product quality testing processes.

How Can You Secure Web Applications?

To understand if the web application is completely secure, you must identify vulnerabilities in the system before an attacker finds out and starts exploiting them. You should test a web application for

vulnerabilities during the entire software development life cycle and not only when the application goes live.

There are various methods to test a web application for vulnerabilities. You can use any of the following methods:

- Use a black box scanner to scan the web application.
- Use a white box scanner to detect issues with the application code automatically.
- Manually audit the source code of the application.
- Do a manual penetration test and security audit.

You cannot use just one method to test the system's vulnerabilities since no method can guarantee a 100 percent detection rate. Every method has its pros and cons.

For example, an automated tool can discover almost all vulnerabilities concerning code compared to a manual tester, but it cannot detect any logical loopholes. The tool cannot think like an attacker and will have an underlying code or application to perform the test. Manual intervention is required to identify logical flaws in the code. Conversely, it can take a lot of time, effort, and money to identify technical loopholes manually, and you cannot guarantee that the manual tester has identified all vulnerabilities in the system.

It is advisable to use every tool available to test a web application if there is no time and budget constraint, but this only happens in an ideal scenario. Therefore, realistically speaking, a business needs to choose the most effective solution regarding time and money to simulate an attack. Most businesses use a black box scanner known as a web vulnerability scanner. It goes without saying that a manual audit should follow an automated web vulnerability scanner. This ensures that both technical and logical vulnerabilities are identified.

Web Vulnerability Scanners

Black Box scanners, also known as web vulnerability scanners, are automated applications that scan websites and web applications for vulnerabilities and other security issues. Web vulnerability scanners became popular because they are easy to use and automate the whole scanning process. If you use a white box scanner, you need to access the underlying code and take the help of someone who understands application development. But with black box scanners, anyone with minimal technical knowledge can operate

the web vulnerability scanner and test a web application.

How do you choose the correct web vulnerability scanner?

The Internet is full of web vulnerability scanners, both for commercial and non-commercial users. It is difficult to choose a scanner that works best for you. Therefore, you must test every scanner available to understand which one suits your application. You must consider multiple aspects before you choose a web vulnerability scanner. The first and obvious question is whether to use a free scanner or one with a commercially paid license? It is recommended that you always use a commercial scanner since they have regular updates, enable support from professionally trained teams, etc.

You can then choose a web vulnerability scanner based on the following criteria.

How well can it identify web application attack surfaces?

When you test the scanner, carefully examine what one has the best crawler. A crawler is a scanner component, which scans the application for all entry points where the attacker can initiate the hack. It is a critical component since it is easier to identify vulnerability only when the entry points are identified.

To understand what crawler is the best, analyze the results given by each crawler. Use the following parameters:

1. The number of pages scanned
2. The number of files used
3. Various parameters included during the scan

There is a possibility that a crawler was unable to scan the entire surface of the web application. This often happens when the crawler must be configured manually, which brings leads to the next point.

User-Friendliness of the Web Vulnerability Scanner

While most black box scanners are automatically configured to scan a web application, some may need you to specify certain parameters manually. Your business does not need to have a dedicated web application security team to configure a web vulnerability scanner as per business requirements. This means that the security scanner should be user-friendly so that anybody with basic programming or technical skills can configure the scanner. User-friendly web vulnerability scanners help businesses save money since they do not have to hire specialists to work on it.

Ability to Identify Vulnerabilities

The next criterion is to see which web vulnerability scanners can identify the maximum vulnerabilities and how many contain false positives. Web vulnerability scanners find thousands of vulnerabilities in a web application, but more than 60 percent of those were false positives.

You may ask why this is a problem? The issue with false positives is that a manual auditor must spend more time trying to verify if the vulnerability is indeed a vulnerability. This is a waste of resources and, therefore, needs to be avoided.

Automation

More automation in a web vulnerability scanner is equal to more relief for the company. This means that a tester need not manually configure each parameter since the scanner is already configured to scan well-known vulnerabilities. There are more vulnerabilities in a web application than what meets the eye. It is practically impossible for people to identify every vulnerability even if there is a time restriction. It is safer to use an automated scanner since it can complete the scan and identify vulnerabilities within two-three hours.

Additionally, a tester's knowledge about any vulnerability in the system is dependent on their experience. An automated web vulnerability scanner is already equipped with knowledge of existing vulnerabilities in web applications, and the developers of that scanner constantly update the database based on newly discovered vulnerabilities in different web applications.

In addition to these technical steps that you can take to secure your web application, you must stay informed. The Internet is full of information with blogs and websites on web application security. You can protect your applications and software better if you update your knowledge and skills regularly and stay abreast of what is going on in the industry.

Smartphone Security

When someone talks about a ransomware attack, people immediately think of attacks on employees using laptops or desktops. This is where an attacker thinks differently. An attacker always considers all possibilities that help them enter the system or network. An easy way to do this is through smartphones, which are easy to hack into and offer quick rewards.

The following are some numbers concerning cybercrimes and

smartphones:

- Reports suggest that the number of attacks on smartphones had gone up by 50 percent in 2019 as compared to 2018. This was not just for Android devices. There is an estimate that, presently, around 1.6 million attack campaigns are targeting Apple devices.
- Reports by the researcher Ponemon suggest that in the past twelve months, 67 percent of small-medium sized businesses are victims of cyberattacks, and 58 percent were victims of a data breach. All this because of inefficient security on smartphones.
- The data breach report presented by Verizon in 2019 showed that 42 percent of the victims were small business owners.
- Forty-seven percent of small-medium sized businesses agreed that they do not know how to secure smartphones to protect their businesses.

Attacking smartphones is getting popular since attackers always look for new ways to attack your business. For instance, even state-sponsored attacks have started integrating smartphones to gather information for their attacks. The reason smartphones are targeted is because everyone takes smartphone security for granted.

Here are the simplest ways users and business owners can protect their smartphones and data:

Update the Operating System and Apps

Just like you would do in the case of your laptop or desktop, it is also important to keep your smartphone's operating system and its applications up to date. Many people are idle about updating their smartphone's operating system and apps. This opens their smartphone up to new vulnerabilities. When operating system and application providers roll out an update, they try to patch any discovered vulnerabilities. For instance, when OnePlus decides to upgrade the system, it sends you a notification. Once you download and install it, it tells you what fixes it made to your phone. Application providers also do the same. There may be a weekly update at times. If you do not update your smartphone, it becomes an easy target for attackers.

Today, businesses also have a Bring Your Own Device BYOD policy where personal smartphones can be connected to the office network. This being said, businesses need to train their employees about the importance of keeping their smartphones up to date.

Lock Your Smartphone

Keeping your phone unlocked is convenient for checking texts, emails, etc., but imagine if you forgot your phone in a coffee shop. What do you think will happen? If you do not have a security code, anybody can pick your phone up and access all your information. If your phone contains business information, you will put your business or organization at risk because of minor negligence.

Therefore, always make it a point to lock your smartphone with a passcode or biometric authentication.

Use Inbuilt Device Security Features

You can use the "locate my device" feature if you misplaced your smartphone. The feature makes your phone ring, which can threaten the thief or help you locate your phone if you lost it temporarily. There are options on the phone even to delete all data if there were a few incorrect passcode attempts.

Using Bluetooth and Wi-Fi Wisely

Many people like to use free or public Wi-Fi. If you are using a smartphone with critical business data, think twice before you do this. Make it a point to ensure that the Wi-Fi you use is from a legitimate network. Free Wi-Fi available across public spaces such as coffee shops, malls, etc. are less secure.

The same goes for Bluetooth. People tend to ignore the Bluetooth feature leaving it on all the time. An attacker can take advantage of this ignorance, and break into your phone if they get sufficiently close to you.

App Permissions

When you install an app on your smartphone, it asks you permission to access certain features on your phone. Be careful before you approve these permissions. For example, it is understood for Google maps to have permission to access your location since it needs this to give you the right information. On the other hand, if a simple game you downloaded asks you for permission for your location, you need to be alert immediately. For all you know, attackers created the game to access your location. An application may ask many other permissions, so make sure to read these permissions before you give the application access.

Phishing and Spam Emails

Your smartphone also has an email application, and therefore, hackers can use phishing to obtain sensitive information. Thus, everything you learned in Chapter Three holds for emails received

on your smartphone.

Data Backups

Data backups are as important for your smartphone as for your laptops and desktops. Some issues may occur at any time. Your smartphone may get stolen, or you may cause accidental damage to it. Therefore, it is advised that you maintain data backup.

Smartphone providers these days even offer automated backups for your data through cloud services such as Google Drive for Android and iCloud for iPhones. Always take advantage of this feature, so you never have to worry about losing your data.

Antivirus Apps

It is good to have an antivirus app installed on your smartphone since it protects your phone from any kind of malware. Attackers always deploy malware first to your device, and so it is best to install an antivirus app to prevent any attacks.

Source of Your Apps

The majority of users ignore this fact, but it is very important that the apps you download come from trusted sources. For Android, the Play-store is a trusted source, and for Apple, the app store. There are certain apps unavailable on the play store or app store, and this is due to security reasons. Users tend to sideload these apps that may be tampered with by an attacker, and your smartphone is conveniently opened up for attack just because of your negligence to sideload third-party apps.

To conclude, smartphones are critical extensions to business, more now than ever, and are no longer just a device used for making phone calls. Given its form factor, you can easily lose it, or it can be robbed. Therefore, it is really important in the modern world to care about the security of your smartphone just as much as you care about your other devices.

Chapter Nine: 9 Security Testing Methods

This chapter looks at the different types of security testing methods. At the end, it will focus more on penetration testing. Most organizations adopt this form of testing to identify any vulnerability in the system and network.

The business maintains cybersecurity testing measures are kept in place to check how prepared they are for any potential attack. A business may have an internal testing team or outsource the security testing to an external team when the need for security testing arises.

Attackers are relentless when they want to perform the attack, and they always look for new loopholes in the system. There are methods such as Penetration Testing, User Awareness testing, Red Team Assessment, etc., that help businesses scan through their infrastructure for loopholes that are otherwise overlooked.

Types of Security Testing

Vulnerability Assessment

The method of vulnerability testing is employed when a business needs to identify drawbacks within their systems, applications, and networks across their infrastructure. The following assets can be reviewed by implementing vulnerability testing:

- Web Applications
- System Builds
- Network Devices
- Network Infrastructure
- Phishing Attack Surfaces
- Mobile Apps

User Awareness Testing

User Awareness Testing, also known as UAT, is when business users test the routine tasks on an application. A business is built on its employees, but as mentioned, they can also be the weakest link to the security of a business process. By implementing user awareness tests and simulating attacks, a business can determine how employees react to a certain kind of attack.

User awareness testing has proved to be effective in identifying both digital and physical vulnerabilities. It helps you understand the level of preparedness against a phishing attack, and what a business can do to educate its employees regarding cybersecurity.

Red Team Assessment

Attackers do not follow any rules, and they do as they please. They know how to use different tools and software to attack the system and network of an organization to steal sensitive information. They may also find a way to disrupt essential services. A Red Team Assessment test helps the organization determine how prepared it is for any attack.

This test covers every attack surface, internal or external, and considers the application layer, network layer, employee awareness, and the physical aspects of security. The test is conducted legally with all required authorizations and uses harmless attack vectors to break into the infrastructure and exploit it in all ways possible.

Members of a red team assessment usually check the following entities for exploits and vulnerabilities.

Physical

Tests check for vulnerabilities at the physical level, such as the office, data centers, warehouses, and other relevant buildings.

Technology

Tests cover all the digital infrastructure. The team also tests personal BYOD and official mobile devices and other network devices such as routers, switches, etc.

People

Tests check internal employees, external contractors, business partners, and other high-risk departments.

After the assessment is completed, a detailed report is created and presented to the management. The management then consults with various cybersecurity experts in the organization to take preventive measures and improve the infrastructure.

Build Review

Build Reviews are tests performed by a dedicated team of security professionals on software every time a new version is rolled out. Build reviews help the organization perform a thorough assessment of every new software build. This helps the team strengthen the software's security further through a feedback loop, ensuring that it is safe from an attack.

The following components are tested as a part of build reviews:

- Servers
- Firewalls
- Active Directory
- Switches
- Routers
- Database Servers
- Application Servers
- Workstations

Penetration Testing

Most organizations adopt this method extensively to address the security concerns of the organization. This section takes you through the process of penetration testing.

Penetration Testing is the process of testing applications to find vulnerabilities. The teams do this by bombarding the network with malicious vectors after prior authorization from a business. The organization simulates an attack similar to a real attack to identify any vulnerability in all surface areas of digital infrastructure.

The purpose of penetration testing is to find any loopholes in a system and patch them before an attacker can access the system without authorization and steal sensitive information.

A penetration test is also known as a pen test and an ethical hacker. It helps determine if the existing defense mechanisms of a system are sufficient to prevent any attacks. Furthermore, there are reports generated after the completion of a penetration test that tell the business what countermeasures they must add to the system and network to prevent any attacks.

A system may have vulnerabilities due to the following reasons:

Error During Design and Development

Nothing is ever perfect, and there are chances of flaws in both software and hardware. The presence of the smallest of errors in software design can expose critical data during an attack.

Bad System Configuration

This can be another reason why there are vulnerabilities in the system. Poorly configured systems may open a backdoor for the attacker to break into the system and steal or destroy data.

Human Errors

There are multiple errors a human can make when they develop the application. They may also make silly mistakes, such as leaving the system unlocked, poor coding of software, leaving the desk and documents unattended, falling prey to phishing scams, etc., which can result in security breaches.

Complexity

The vulnerability of a system is directly proportional to the complexity of the system. An attacker is likely to find more surfaces for attack if the system has many features.

Connectivity

It becomes child's play for an attacker to break into a system connected to an unsecured or open network.

Passwords

The utility of a password is to prevent unauthorized access to something. Passwords need to be complex to avoid random guessing. Organizations must develop a robust password policy. It is also important to change your password regularly and not share them with anyone. These are the basics of securing a password, but despite this, people still share their passwords or write them down on paper and forget about it, and use weak passwords.

Inputs from Users

You may have heard of terms such as buffer overflow, SQL injection, etc. Users give different inputs when they use an application, and a hacker can use these input systems to harm the system.

Management

There is a lot of cost and effort involved in managing the security of systems. If the organization does not have a proper process in place to manage risk, the systems will be vulnerable and easy for a hacker to attack.

Insufficient Training

When the organization does not train its employees and other technical staff, it can cause some errors.

Communication

Communication channels, such as the Internet, mobile networks, telephones, have opened up new media for attacks.

Penetration Testing Tools and Providers

There are automated tools available in today's market to help

you identify standard vulnerabilities. Pen test tools scan code to see if any malicious code lines can result in a security breach. They also validate encryption techniques and find any loopholes in the system or network. Additionally, they also test for hardcoded values in code, such as the username and password.

You should consider certain criteria before selecting a penetration testing tool. They should at least satisfy the following requirements:

- They should be user-friendly and, therefore, easy to use, configure, and deploy.
- They should be able to scan your system irrespective of how complex it is.
- The reports generated by the tool should be able to classify the threats based on severity level. This will help you prioritize your fixes.
- It should be capable of verifying vulnerabilities automatically.
- It should also re-verify any exploits found in the past scans.
- The tools should be able to do detailed logging and reporting.

Once you narrow down the kind of tests your infrastructure requires, you can train internal employees or external consultants to use these security tools. The following is a set of known tools used in penetration testing worldwide.

Nmap

Nmap is an open-source tool. It is used to scan a network and retrieve information about a network. Simply put, Nmap makes use of IP packets to gain information about the following:

- The number of hosts available on a network
- The services offered by those hosts
- The operating system of the hosts
- The firewalls used by the hosts
- And lots of other important information

It is supported on all operating systems and was originally developed for mass scanning of networks, but it works well on single hosts too.

Wireshark

Wireshark is again a free tool used to analyze networks. It gives you a microscopic view of the network's activities and is therefore

used extensively by businesses, governments, and educational institutions.

Acunetix

Acunetix is a penetration testing tool used by software engineers and security professionals since it has numerous features. It is user-friendly, robust, and straightforward. In addition to using internal tools, a business may also directly outsource its penetration testing to leading security companies, some of which are mentioned below.

ScienceSoft

ScienceSoft is a recognized company in the information technology domain for its software services. However, it also takes an interest in providing cybersecurity solutions to companies. The company has been on the market for seventeen years and is experienced in all penetration testing methods, namely, white box, black box, and grey box. This company can test small, medium, and large businesses.

You can contact the cybersecurity team of ScienceSoft to get any assistance in setting up a penetration test for your business.

ImmuniWeb

Based out of Geneva, Switzerland, ImmuniWeb is another well-known penetration testing company. Their penetration testing platform boasts of a DevSecOps feature, which combines people and artificial intelligence to test the system. It also commits to a zero false-positive SLA. Additionally, they also claim they have detected the highest number of vulnerabilities detected and effective reporting. They have a comprehensive set of tools for penetration testing and also include APIs, IoT devices, mobile, and web testing, etc.

They have the following key features:

- Detection of new code in a continuous fashion.
- Manual testing at affordable pricing.
- Patching with single clicks.
- 24/7 support.
- CI/CD integrations for DevSecOps.
- Instant integration.
- Multi-resource dashboard.

Why Penetration Testing?

You may be wondering why this chapter is focusing more on

penetration testing. The WannaCry ransomware that hit the world in 2017 has already been discussed. It was responsible for locking out more than two lakh users out of their computers and demanded money to unlock the systems. It affected many businesses around the world. Penetration testing could have helped these businesses prevent this magnitude of an attack since these tests, when conducted regularly, report the loopholes in security.

Penetration testing majorly helps with the following scenarios:

- Securing user data.
- Identifying vulnerabilities in an application.
- Determining the impact on business in case of a successful attack.
- Helping a business meet compliance concerning security.
- Many IT clients have started asking for penetration tests to be included in the software release life cycle.
- Much financial data is transferred between systems today, and it needs to be secured.

User data is the biggest currency in the world, and loss of such data can cause monetary and reputation damage to an organization. For instance, picture someone hacking a social media website like Facebook, hacking its user database, and exposing those details publicly on the Internet. Facebook can face legal consequences if that ever happened. Therefore, many businesses now enroll for compliance certifications before making financial transactions through their websites.

Some of these compliance certifications include:

- PCI DSS (Payment Card Industry Data Security Standard)
- ISO/IEC 27002, OSSTMM (The Open Source Security Testing Methodology Manual)
- OWASP (Open Web Application Security Project)

Types of Penetration Testing

Social Engineering Test

Social Engineering has already been detailed in Chapter Six, so you already know that social engineering attacks are executed to trick people into disclosing sensitive information about themselves or their organization. Thus, humans can be the weakest link in a security system.

Social engineering tests are conducted by emulating a social

engineering attack. An employee is called via phone or contacted via a medium like text or email, and a scenario is put forward to try and test if the employee ends up disclosing any information. If the test is positive, it will be documented, and steps will be taken to educate employees about it.

Web Application Test

As discussed, various software tools are used to test how secure the code of a web application is. They test the code for any vulnerability and find a way to patch them to prevent any attacks. The team performing this test writes a report that discloses the flaws, and the development team can fix them as soon as possible.

Physical Penetration Test

Many organizations have physical devices on their property and must ensure that only authorized personnel can access the stored devices. This is more so in government and military facilities. All network-related devices and physical entry points are tested for any vulnerabilities. This test is not very relevant to software testing as such.

Network Firmware Testing

Networks are the most important part of an organization's digital infrastructure. Therefore, tests are conducted on all the entry points of a network, and these tests check the traffic going in and out of the point. This test can be conducted both locally and remotely.

Client-Side Testing

During these tests, the organization tests the software on the client's infrastructure to identify any vulnerability in the system.

Wireless Network Testing

As the name suggests, this test will scan all the Wi-Fi hotspots in an organization for vulnerabilities.

The Penetration Testing Lifecycle

The organization follows a disciplined process when it conducts a penetration test. Here is the process:

Data Collection

The first stage of a penetration testing life cycle is the collection of data. Penetration testers use numerous methods to collect information on the target system. The methods may use either a simple or complex tool or application to collect the data. Pen testers may also inspect the source code of the website to gather data

about the target system. Simply put, any information about the target system available publicly is useful and documented. There are several paid and free tools available that the organization can use to collect information about the target system.

Vulnerability Assessment

The data collected in the first stage is analyzed and used to identify the target system's weaknesses. Penetration testers now attack specific attack surfaces to identify any vulnerability. They may conduct these tests using trial and error.

Exploitation

Based on the information collected in the first and second stages, the hackers can use different tools to access the system and exploit it. The exploit could be of any type. A penetration tester may steal data, modify it, or destroy it. Given this is an ethical test, data is usually never destroyed as the tests are conducted against production servers.

Maintaining Access

The next stage is about maintaining access. A hacker does not exploit a system repeatedly since it may trigger the alarm. So, they usually access the system or network once and then deploy tools to maintain their connection to the target system. A penetration tester needs to cover this possibility and emulate the different ways an attacker can maintain access to the system so that they can patch those loopholes.

Reporting

The final stage of the penetration testing life cycle is reporting. Extensive and detailed reports are to be created of tests performed, vulnerabilities found, and steps the organization can take to patch these vulnerabilities. The team must present the report to the senior management of the company, describing the tests and assessments carried out. This report helps the management understand the priority of infrastructure security and invest the required time, effort, and money to secure the business against an actual attack.

To conclude, security testing is a mandatory part of a software delivery life cycle, and organizations should never neglect this process. It costs a bit but definitely helps the business secure its assets against high-level cybercrimes.

Chapter Ten: Skills Required for a Career in Cybersecurity

You are nearing the end of this book, and thus far, you have learned a lot about cybersecurity. So, what next? It is good to have all this knowledge, but what should you do if you wanted to use it? This chapter looks at the careers available in cybersecurity and the skills you need to develop to pursue such a career. The classification of the roles in this chapter will help you decide what area you would like to work in.

A career in cybersecurity is not a bed of roses; it can be stressful. However, it has its rewards. Cybersecurity professionals find themselves in different roles across the organization, but their objective remains the same. They must develop methods and tools to protect the organization's data from any attack.

The process of getting into a cybersecurity role in the industry is not always straightforward. Some people jump into it right out of college, while others like to get some experience in software engineering before choosing to move to a role focused more on security.

Here are some career options available in the cybersecurity field based on the experience of the candidate:

Entry-Level Roles

- Systems Administrator
- Systems Engineer
- Web Developer
- IT Technician
- Network Engineer
- Security Specialist
- Mid-Level Roles
- Security Analyst
- Security Technician
- Incident Analyst
- Cyber Security Consultant
- IT Auditor

● Penetration Tester

Senior Level Roles

● Cyber Security Architect
● Cyber Security Manager
● Cyber Security Engineer
● Chief Information Security Officer

Four Popular Careers in Cybersecurity and How to Get There

Security Architect

If you like to solve problems, and develop strategies to prevent the same problems, consider the role of a security architect.

A security architect is responsible for designing, developing, and implementing security for an organization's systems and networks. They are capable of developing efficient complex security structures. The security structures can prevent any malware, DDoS, and other attacks.

The average salary for a security architect in the USA is around $120,000 per annum. Security architects must have at least five years of experience in the IT industry and three to five years in security.

Follow the path given below if you wish to pursue a career as a security architect:

● Pursue a degree in information technology, computer science, cybersecurity, or any other relevant field. Alternatively, you can earn equivalent industry-level certifications.

● Enter the industry as a systems administrator, security administrator, or network administrator.

● Work in the same organization for a while, and move up the organization until you reach a security engineer level.

● At this point, you can switch to a security architect role.

The responsibilities of a security architect are as follows:

● Research about current attack trends and design security architecture for all IT projects of the business.

● Provide the requirement to management for networks and network devices.

● Perform security testing, such as risk analysis and

vulnerability testing.

● Research about the latest standards in security and implement them in the organization.

Training

The role of a security architect is a senior-level role, and therefore recruiting managers to look for specific certifications when they hire any candidate. Industry-level certifications in cybersecurity give your profile an edge over your competitors. You can first earn a CompTIA Security+ certificate and then proceed to the Certified Ethical Hacker (CEH) certification.

To move on to the advanced and expert levels, you can earn an EC-Council Certified Security Analyst (ECSA) certification and Certified Information Systems Security Professional (CISSP) certification.

Security Consultant

A security consultant, also known as a cybersecurity expert, knows everything there is to know about cybersecurity. They can analyze risks and problems and provide appropriate solutions to other organizations to secure their infrastructure and protect their data. Some organizations use a different name for this role. Some commonly used terms are security consultant, network security consultant, or database security consultant.

A security consultant is expected to be versatile and able to answer any queries related to cybersecurity. The salary range depends on the experience, but a senior-level security consultant can make up to $106,000 per annum in the USA. Most organizations prefer to hire consultants with at least three to five years of experience.

You can follow the path below to become a security consultant:

● Pursue a degree in information technology, computer science, cybersecurity, or any other relevant field. Alternatively, you can obtain the equivalent industry-level certifications.

● Enter the industry though a general IT role.

● Continue to work in the same organization and move up the ladder until you reach the security administrator, auditor, or analyst roles.

● Get yourself some industry-level certifications and improve your skills.

● Try moving to a security consultant role.

The daily tasks of a security consultant are as follows:

- Determine ways to protect systems, networks, and data from attacks.
- Perform security assessments and vulnerability tests.
- Communicate with staff and employees to understand security issues.
- Using industry-standard solutions to test security.
- Supervise and guide the security team of the organization.

Training

You can start with the CompTIA Security+ certificate and move on to the Certified Ethical Hacker (CEH) certification. You also need to earn the Cybersecurity Analyst (CySA+) certification.

Advanced certifications include Certified Information Systems Auditor (CISA), EC-Council Certified Security Analyst (ECSA), and Certified Information Security Manager (CISM). To get to the expert level, you can get certified with Certified Information Systems Security Professional (CISSP).

Ethical Hacker/Penetration Tester

Penetration testers, also known as ethical hackers, understand how an attacker thinks, and use that understanding to simulate different attacks on the organization's systems and network to prevent any malicious attacks. They perform this attack only with the management's consent, identifying the weak spots before an attacker can exploit them. This helps the business to protect their sensitive and critical data, both in storage and in transit.

The average salary of a penetration tester in the USA is $80,000 per annum.

If you want to become a penetration tester, follow the career path given below.

- Pursue a degree in information technology, computer science, cybersecurity, or any other relevant field. Alternatively, you can obtain the equivalent industry-level certifications.
- Enter the industry as a systems administrator, security administrator, or network administrator.
- Get yourself some industry-level certifications and sharpen your skills.
- Continue to work in the organization until you move up the organization and earn a senior penetration tester, security architect,

or security consultant role.

The duties of a penetration tester are as follows.

- Conduct penetration tests on applications, systems, and networks.
- Analyze weaknesses to identify methods an attacker could use to exploit the system.
- Discuss and document the findings with the IT teams.
- Design and implement new tools for penetration testing to keep up with modern-day attacks.

Training

Start with the CompTIA Security+ and move on to the Certified Ethical Hacker (CEH) certification. At an advanced level, you can earn the CompTIA Advanced Security Practitioner (CASP) and EC-Council Certified Security Analyst (ECSA). To become an expert, you can earn the Certified Information Systems Security Professional (CISSP).

Chief Information Security Officer (CISO)

The Chief Information Security Officer profile is a senior-level profile in the field of cybersecurity. It is a very respected and rewarding job and includes a lot of power and freedom concerning creativity. The Chief Information Security Officer is responsible for assembling a security team and keeping a macroscopic view over the organization's security. The CISO will report to the CEO of the organization.

The average salary of a CISO is around $160,000 per annum in the USA. You must have at least seven to ten years of experience in the cybersecurity domain, and five years out of those must include managing security teams.

You can achieve the career level of a CISO by:

- Pursuing a bachelor's degree in information technology, computer science, cybersecurity, or any other relevant field. Alternatively, you can earn any equivalent industry-level certifications.
- Enter the industry as an analyst or a programmer.
- Continue to work in the organization until you move up the ladder to become an engineer, auditor, consultant, or security analyst.
- Get yourself some industry-level certifications and sharpen

your skills.

- Try to become a manager of a team dealing with security.
- Get an MBA degree with a focus on IT.
- Get promoted to the role of Chief Information Security Officer (CISO).

You will be the head of the IT team, and your responsibilities will be as follows:

- Taking the last round of interviews to have the best team of IT security experts.
- Creating new plans for security project deployments and working on improving existing methods.
- Analyzing and approving the design and development of security policies proposed by the IT and security teams.
- Establishing programs for risk management by collaborating with other leaders in the organization.
- In the event of a breach, the CISO must take charge of the security teams and propose a plan of action to fix and prevent the breach in the future.

Training

When you start your journey off in the information security industry, you must obtain the Certified Information Systems Auditor (CISA). At the advanced level, obtain the Certified Information Security Manager (CISM) and become an expert by completing Certified Information System Security Professional (CISSP).

Required Skillset for a Career in Cybersecurity

Here are some skills that recruiters look for when they hire people from the cybersecurity industry.

Soft Skills

Leadership

A security expert leads a team through its ethics, credibility, and responsiveness. With amazing communication skills, a security expert can gain the trust and respect of senior management. It is also important to understand both the internal and external risks of the organization. Security leaders present all key information to the management and drive the business forward through informed decisions.

Always Learning

A security expert must keep up to date on the latest trends in

attacks and solutions for those attacks. An aptitude for learning proves helpful for your personal and professional growth. Security is always evolving in the IT industry, and it requires someone who is a quick learner and can keep up.

Determination

The landscape of threat environments is always changing, and this demotivates some security experts easily. If you do not know how to tackle an attack, do not give up. Persevere and find a way to solve the issue. Determination and persistence always help you solve the issue. An ideal security expert always works on identifying a solution for any problem until the end and does not give up midway.

Collaboration

You must understand that cybersecurity is a shared responsibility of business. There are multiple teams involved, such as application developers, network engineers, server admins, management, and more. You must ensure you collaborate with every team in the organization and respect their inputs, as every input can be useful. Also, when you bond with stakeholders, you can explain the importance of and need for security. Ensure that every department in the organization does not ignore security.

Analytical and Insightful

A skilled security expert is good at analyzing incoming attacks and can assess how they can be thwarted. They further understand the attack surfaces and their vulnerabilities to minimize the attacks in the future. It can take a few years to develop this skillset, and sometimes it's also an intuition that helps a few individuals.

Hyper Critical Thought Process

A skillful security expert knows how the attacker thinks. This helps them visualize how the attacker may plan and execute the attack. Therefore, they know how to think like the attacker and conduct penetration tests to identify vulnerabilities in the system before the attacker uses them to exploit the system and network.

Approachable

A security expert has to communicate with other teams constantly. Sometimes other teams may even want to consult the security expert before making changes to network policies or code. Thus, you must be approachable so that other leaders and team

members can consult you. The combined effort helps the business strengthen its network and security policies.

Project Manager

Since you are a cybersecurity leader, you work day in and day out to protect your organization against attacks. You must develop holistic solutions rather than going with a solution for every attack module.

Technical Skills

Incident Management and Response

As a security expert, you are expected to handle any threat that violates the organization's security in real-time. There could be an incident involving malware, phishing, ransomware, etc., and it is critical that you can handle the situation, resolve it, and prevent it from happening again.

SIEM Management

SIEM stands for Security Information and Event Management. There are tools and services part of SIEM, and a security expert is expected to be well versed with them. You must learn to automate security procedures using SIEM tools so that the organization translates real-time alerts to response plans to prevent the effect.

Firewall

A security expert must thoroughly know the ins and outs of the firewall configuration so that it becomes easier to filter out malicious traffic from the network. Additionally, they must be very knowledgeable about intrusion detection and intrusion prevention systems and how they could be used in combination with the firewall.

Intrusion Detection

You are expected to know the workings of the intrusion detection system thoroughly so you can leverage it against any attack.

Application Security

A good security expert can find loopholes in the application and fix them before an attack comes in. It is also good practice to test applications during the software development life cycle to identify any vulnerability and fix them before deploying the application into production.

Malware Prevention

A good security expert can identify advanced persistent threats that may bypass traditional security solutions, such as firewalls, antivirus, etc.

Mobile Device Management

A security expert must work with the IT team to explain how hackers can exploit mobile devices such as smartphones, laptop, tablets, etc., to breach the system. They should further discuss how these devices could be secured to prevent a security breach.

Data Management

Data is the most expensive asset for any business, and a security expert should manage and protect it at all costs.

Digital Forensics

A security expert should know about digital forensics and leverage forensic tools to find anomalies in data or the network, which can be a backdoor for an attacker. They should subsequently patch the data or network if any anomalies are found.

Identity/Access Management

Through identity and access management, the organization creates roles, classifies users into groups, and then assigns roles to them. The IT team defines these roles along with the management, and a security expert is expected to audit the access levels granted to users and groups in the organization regularly.

Intelligence and Analytics

A security expert must know how to use analytics to understand historical attack patterns and learn how to predict future attacks and be ready for them. Reports suggest that if analytics is leveraged to combine network data and application data, it can help prevent attacks.

Audit and Compliance

While securing systems and networks, a security expert needs to ensure that all regulatory compliances such as PCI DSS, SOC, GDPR, HIPAA, PCAOB, SOX, etc., are adhered to by the organization. Compliance and security audits are critical since non-adherence to regulatory compliance can attract huge penalties or fines from the government.

Conclusion

Cybercrimes are happening every second on the Internet. Cybercriminals are constantly planning a crime, regardless of whether it is for monetary gains or to disrupt the peace of the digital world. Therefore, cybersecurity is more relevant than ever today. Businesses must protect themselves from various kinds of attacks that hackers can launch on their systems and network. Hopefully, upon completing this book, you have sufficient knowledge to protect yourself and your business from modern-day cybercrimes.

At the same time, this book might have inspired you to take up a career in cybersecurity. The demand for cybersecurity professionals has increased in the last few years since the number and types of cybercrimes have significantly increased. Recruiters in all industries find it very difficult to find the right talent for this job, and this gives anyone with the right skills and qualifications a huge opportunity. There is also a sense of urgency to fill these positions as cybercriminals are constantly planning a new attack and never take a holiday themselves.

This book has taken you through everything you need to know as a beginner in the cybersecurity domain and how to start planning if you want to take it up as a career. You have also learned enough to keep yourself protected on the Internet.

References

https://www.forcepoint.com/cyber-edu/cybersecurity
https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#~how-cybersecurity-works
https://www.cybintsolutions.com/20-cyber-security-terms-that-you-should-know/
https://list25.com/25-biggest-cyber-attacks-in-history/
https://www.varonis.com/blog/cybersecurity-careers/
https://www.newhorizons.com/article/4-cybersecurity-career-paths-and-the-training-to-get-you-there
https://cipher.com/blog/the-must-have-skill-sets-certifications-for-cyber-security-careers/
https://www.integrity360.com/cyber-security-testing
https://www.softwaretestinghelp.com/penetration-testing-guide/
https://www.netsparker.com/blog/web-security/getting-started-web-application-security/
https://www.zdnet.com/paid-content/article/protecting-your-mobiles-from-a-rise-in-cybersecurity-attacks/
https://www.businessnewsdaily.com/11197-protect-your-smartphone-from-hackers.html
https://www.forcepoint.com/cyber-edu/network-security
https://www.coxblue.com/how-to-protect-your-business-from-cyber-attacks-2/
https://www.tetradefense.com/cyber-risk-management/13-ways-to-protect-your-business-from-a-cyber-attack-in-2019/
https://security.berkeley.edu/resources/best-practices-how-to-articles/top-10-secure-computing-tips